UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO EM DIREITO

A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NOS PAÍSES DO MERCOSUL EM FACE DA SEGMENTAÇÃO COMPORTAMENTAL: um estudo comparado.

DISSERTAÇÃO DE MESTRADO

Felipe Stribe da Silva

SANTA MARIA, RS, BRASIL.
2015

A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NOS PAÍSES DO MERCOSUL EM FACE DA SEGMENTAÇÃO COMPORTAMENTAL: um estudo comparado

Felipe Stribe da Silva

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-graduação em Direito, na Área de Concentração Direitos Emergentes na Sociedade Global, com ênfase na Linha de Pesquisa Direitos na Sociedade em Rede, da Universidade Federal de Santa Maria (UFSM), como requisito parcial à obtenção do grau de
Mestre em Direito

Orientadora: Prof.ª. Dr.ª Rosane Leal da Silva

SANTA MARIA, RS, BRASIL.
2015

Universidade Federal de Santa Maria
Centro de Ciências Sociais e Humanas
Programa de Pós-Graduação em Direito
Mestrado em Direito

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NOS PAÍSES DO MERCOSUL EM FACE DA SEGMENTAÇÃO COMPORTAMENTAL: um estudo comparado

elaborada por
Felipe Stribe da Silva

como requisito parcial para obtenção do grau de
Mestre em Direito

COMISSÃO EXAMINADORA

Rosane Leal da Silva, Drª.
(Presidente/Orientador)

Letícia de Campos Velho Martel, Drª. (PUC RS)

Rafael Santos de Oliveira, Drº. (UFSM)

Santa Maria, 09 de Março de 2015.

AGRADECIMENTOS

A Andressa, eterno amor da minha vida, que me fez entender o sentido do tempo presente, fazendo com que eu perceba que o melhor futuro que eu poderia sonhar seria ao seu lado.

Ao meu pai Rudnei Freitas da Silva, exemplo de homem e de trabalhador, que me ensinou os valores da honra, do respeito e da importância de fazer sempre o melhor em todas as minhas atividades, e por ter auxiliado de todas as formas os meus primeiros passos no estudo do Direito.

A minha mãe Mari Rubia Stribe da Silva por ter sempre os braços abertos, para um momento de carinho, e para me mostrar que todas as dificuldades são superáveis se eu acreditar que consigo e me dedicar, e por ter auxiliado de todas as formas os meus primeiros passos no estudo do Direito.

Ao colega de Assessoria Jurídica e amigo Dr. Cláudio Alves Malgarin, um verdadeiro mestre na perfeita acepção do termo, sempre pronto a aconselhar e auxiliar em minhas escolhas profissionais e acadêmicas.

A colega de Assessoria Jurídica e amiga Liana Araújo, pelo apoio e auxilio para cumprir todas as obrigações de meu cargo e ao mesmo tempo dedicar o tempo necessário aos meus estudos.

Ao Centro Universitário Franciscano, instituição de renome a qual eu tenho a honra de integrar os quadros funcionais, e de quem sempre recebi total apoio nos meus estudos. Um agradecimento especial às irmãs Irani Rupolo, reitora, e Inacir Pederiva, pró-reitora de administração, pelo exemplo de dedicação, empreendedorismo e respeito aos valores humanos e franciscanos no tratamento de seus funcionários.

A minha orientadora Profª Drª Rosane Leal da Silva, exemplo de acadêmica e de profissional, sempre encontrando tempo e paciência para revisar os meus escritos e debater as idéias centrais deste trabalho, ensinando que assim como as atividades docentes tradicionais, a orientação acadêmica exige além de conhecimento técnico e científico, talento para compreender e respeitar as idéias do outro.

Ao programa de pós-graduação em Direito – Mestrado em Direito e a todos os docentes que auxliaram a ampliação dos meus horizontes acadêmicos com suas disciplinas e artigos, além de ensinar que a carreira acadêmica exige extrema dedicação. E a todos os meus colegas da primeira turma, pela amizade e respeito no debate e na troca de idéias, este último pressuposto essencial para o desenvolvimento da ciência jurídica.

RESUMO

Dissertação de Mestrado
Mestrado em Direito
Programa de Pós-Graduação em Direito
Universidade Federal de Santa Maria

A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NOS PAÍSES DO MERCOSUL EM FACE DA SEGMENTAÇÃO COMPORTAMENTAL: um estudo comparado

AUTOR: FELIPE STRIBE DA SILVA
ORIENTADORA: ROSANE LEAL DA SILVA
Data e Local da Defesa: Santa Maria, de Março de 2015.

O presente trabalho tem como objetivo investigar o tratamento jurídico conferido aos dados pessoais nos ordenamentos jurídicos da Argentina, Uruguai e Brasil, discutindo se suas legislações são eficazes para evitar a prática da segmentação comportamental ocorrida na Internet. Esta estratégia de marketing é utilizada por muitas empresas e apresenta forte potencial ofensivo aos direitos fundamentais dos internautas, especialmente o direito à privacidade, o que suscita novos conflitos emergentes da sociedade em rede. Apesar dessas novas situações de vulnerabilidade ao direito à privacidade, o Brasil é o único país do Mercado Comum do Sul (MERCOSUL) que ainda não conta com legislação específica sobre a proteção de dados pessoais (tangencialmente tratado pelo Marco Civil da Internet), diferentemente de Estados como Argentina e Uruguai, cuja legislação foi considerada com um nível de proteção adequado pela União Europeia, uma das precursoras no estudo dessa temática. Diante dessa assimetria nos ordenamentos jurídicos questionou-se: Qual o grau de proteção que estas legislações concedem ao cidadão internauta? Este maior grau de proteção legislativa surte um relfexo alterando significativamente nas políticas empresarias dos intermediários da Internet, gerando Termos de Política de Privacidade mais protetivos? Para responder a esses problemas de pesquisa foi composto um marco teórico que reúne as contribuições de reconhecidos autores da área, como Antonio Enrrique Perez-Luño, Stefano Rodotá e Manuel Castells, eleitos por sua produção discutir as profundas alterações da sociedade desencadeadas pela massiva utilização das Tecnologias da Informação e da Comunicação (TIC). Como forma de solucionar a problemática apontada optou-se pela utilização de abordagem dedutiva, complementada pela adoção do método do procedimento comparativo, partindo-se da compreensão ampla de autodeterminação informativa, de sociedade informacional e de segmentação de comportamentos para a análise específica das legislações dos países investigados e dos Termos de Políticas de Privacidade lá utilizados pelo Provedor de Acesso TERRA. Tais métodos foram complementados pelas técnicas de pesquisa bibliográfica e documental. Após a análise constatou-se que a existência de legislação específica sobre a proteção de dados pessoais na Internet amplia a proteção do titular dos dados pessoais, privilegiando o exercício da sua autodeterminação informativa, como ocorre com as legislações da Argentina e do Uruguai, e, por outro lado, a ausência de tal regulamentação tende a dificultar o exercício do controle pelo titular da destinação dos seus dados pessoais. Como decorrência dessa assimetria de proteção, verificou-se que os intermediários do acesso à Internet, dentre os quais o provedor "Terra", tendem a documentar a sua política de privacidade de forma diferenciada nestes locais, fato que aponta para a maior vulnerabilidade dos internautas brasileiros e corrobora a necessidade de edição de legislação específica sobre o tema no Brasil.

PALAVRAS-CHAVE: Autodeterminação Informativa, Dados Pessoais, Segmentação de Comportamentos, Tenologias da Informação e Comunicação, Termos de Política de Privacidade.

RESUMEN

Disertación de Maestría
Maestría en Derecho
Posgrado en Derecho
Universidad Federal de Santa Maria

LA PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN LOS PAÍSES DEL MERCOSUR EN FACE DE LA SEGMENTACIÓN COMPORTAMENTAL: un estudio comparado

AUTOR: FELIPE STRIBE DA SILVA
ORIENTADORA: ROSANE LEAL DA SILVA
Fecha y lugar de la defensa: Santa Maria, de Marzo de 2015.

El presente estudio ten como objetivo investigar el tratamiento jurídico conferido a los datos personales en los ordenamientos jurídicos de la Argentina, Uruguay y Brasil, discutiendo si sus legislaciones son eficaces para evitar la práctica de la segmentación comportamental ocurrida en internet. Esta estrategia de marketing es utilizada por muchas empresas y presenta fuerte potencial ofensivo a los derechos fundamentales de los internautas, especialmente el derecho a la privacidad, lo que suscita nuevos conflictos emergentes de la sociedad en red. A pesar de esas nuevas situaciones de vulnerabilidad al derecho a la privacidad, el Brasil es el único país del Mercado Común del Sur (MERCOSUR) que aún no cuenta con legislación específica acerca la protección de datos personales (tangencialmente tratado por el Marco Civil de la Internet), diferentemente de Estados como Argentina y Uruguay, cuya legislación fue considerada con un nivel de protección adecuado por la Unión Europea, una de las precursoras en el estudio de esa temática. Delante de esa asimetría en los ordenamientos jurídicos se cuestionó: ¿Cuál el grado de protección que estas legislaciones conceden al ciudadano internauta? ¿Esté mayor grado de protección legislativa refleja alterando significativamente en las políticas empresarias de los intermediarios de la Internet, generando Términos de Política de Privacidad más protectivos? Para responder a esos problemas de investigación fue compuesto un marco teórico que reúne las contribuciones de reconocidos autores del área, como Antonio Henrique Perez-Luño, Stefano Rodotá y Manuel Castells, elegidos por su producción discutir las profundas alteraciones de la sociedad desencadenadas por la masiva utilización de las Tecnologías de la Información y de la Comunicación (TIC). Como forma de solucionar la problemática apuntada se optó por la utilización de abordaje deductivo, complementada por la adopción del método del procedimiento comparativo, partiéndose de la comprensión amplia de autodeterminación informativa, de sociedad informacional y de segmentación de comportamientos para el análisis específico de las legislaciones de los países investigados y de los Términos de Políticas de Privacidad allá utilizados por el Proveedor de Acceso TIERRA. Tales métodos fueron complementados por las técnicas de investigación bibliográfica y documental. Después del análisis se constató que la existencia de legislación específica sobre la protección de datos personales en internet amplía la protección del titular de los datos personales, privilegiando el ejercicio de su autodeterminación informativa, como ocurre con las legislaciones de la Argentina y de Uruguay, y, por otro lado, la ausencia de tal reglamentación tiende a dificultar el ejercicio del control por el titular de la destinación de sus datos personales. Como decorrencia de esa asimetría de protección, se verificó que los intermediarios del acceso a la Internet, de entre los cuales el proveedor “Tierra”, tienden a documentar su política de privacidad de forma diferenciada en estos locales, hecho que apunta para la mayor vulnerabilidad de los internautas brasileños y corrobora la necesidad de edición de legislación específica sobre el tema en Brasil.

PALABRAS CLAVE: Autodeterminación Informativa, Datos Personales, Segmentación de Comportamientos, Tecnologias de la Información y Comunicación, Términos de Política de Privacidad.

SUMÁRIO

INTRODUÇÃO

A estrutura social do sistema capitalista, após a década de 70 do século XX, foi profundamente alterada pelo desenvolvimento e utilização massiva das Tecnologias da Informação e da Comunicação (TIC), e passou a ser identificada como uma "sociedade informacional"[1].

Tal sociedade, além de prezar pela informação, passou a tornar o fluxo desta algo essencial para os processos de comunicação. Este fluxo ocorre em um ambiente não físico, denominado *ciberespaço*, contudo o acesso a este local exige do indivíduo determinadas condições econômicas e técnicas, dentre estas, exige um provedor de acesso à *Internet*.

O acesso ao espaço onde ocorrem estes fluxos torna-se essencial na maioria das áreas da vida dos indivíduos, tendo em vista que a contemporaneidade tende a concentrar e mesclar as diferentes relações econômicas, familiares, culturais, políticas e sociais no *ciberespaço*.

Considerando-se que a rede mundial de computadores (*Internet*) opera segundo a lógica do intenso fluxo de dados pessoais, empresariais, públicos, dentre outros, estes dados geralmente não estão ordenados, apresentando-se particionados, segmentados por categorias. Não obstante, é simples obter determinados dados relacionados a um objetivo específico, basta intermediar um filtro de acesso.

Esses filtros trazem visíveis vantagens aos indivíduos, pois evitam o acesso de crianças e adolescentes a conteúdo pornográfico, possibilitam a exclusão de conteúdos decorrentes de discurso de ódio, além de permitiremàs empresas, cujo serviço é o acesso, verificar a qualidade do sinal de conexão e realizar reparos técnicos para melhor prestar o serviço contratado.

Mas ao lado dessas vantagens aos usuários, surgem os riscos, dentre os quais o de violação aos seus direitos fundamentais, como, por exemplo, o uso de filtros de acesso para obter dados pessoais destes internautas com a finalidade de, a partir das informações, refletir seus comportamentos e, criar perfis que reflitam suas personalidades, para lhes direcionar uma publicidade.

Essas e outras situações de vulnerabilidade aos Direitos Fundamentais, somadas ao avanço das TIC, também exigiu que o princípio da proteção à privacidade tivesse o seu sistema de regulamentação repensado a partir de um direito específico: a proteção de dados pessoais.

---

[1] Expressão inicialmente cunhada por Manuel Castells na obra "Sociedade em Rede" (2003-A).

Considerando esse novo contexto, propõe-se a discussão da temática da proteção dos dados pessoais em face da segmentação comportamental, situação muito comum e por vezes invisível ao titular de direitos.

Essas estratégias empresariais ocorrem porque a comercialização de produtos e a prestação de serviços referentes às tecnologias informacionais é considerada um interessante setor da economia, sendo que as empresas de telecomunicações se interessam sobre este campo, destacando-se as empresas que atuam para promover o acesso à *Internet*. Todavia, a necessidade de atualização constante das tecnologias na prestação destes serviços, bem como a exigência de ampliação dos pontos de conexão, acabou por concentrar a atuação nesse segmento em algumas poucas grandes empresas.

Para ingressar no mundo virtual os indivíduos disponibilizam os seus dados pessoais a estes grandes provedores de acesso à *Internet*, que atuam em um setor cada vez mais concentrador de poder.

As principais empresas que atuam neste setor disponibilizam determinados termos/políticas de privacidade, que são documentos onde o provedor expressa a forma como pretende tratar os dados pessoais dos usuários obtidos durante a prestação dos seus serviços.

Até o corrente ano, o ordenamento jurídico brasileiro tinha uma completa lacuna legislativa, sobretudo se comparado aos países vizinhos, membros do Mercado Comum do Sul (Mercosul) Argentina, Paraguai e o Uruguai, que já regulamentaram o tratamento e a proteção de dados pessoais na *Internet* na década passada. Porém, com a Lei nº 12.965, de 23 de Abril de 2014 (Marco Civil da *Internet*), tal temática passou a ser tangencialmente regulamentada no Brasil, embora a proteção de dados pessoais, especificamente, ainda não conte como lei tendo havido somente projeto de lei que visava regulamentar de forma precisa a matéria, mas que já foi arquivado.

Todos os demais Estados, membros iniciais quando da fundação do Mercosul[2] têm legislação específica de proteção de dados: a Argentina conta com a Lei nº 25.326/2000, o Paraguai, por sua vez, tem a Lei nº 1.969/2002 e, por fim, o Uruguai regulamenta a matéria a partir da Lei nº 13.331/2008.

Destas, apenas as Leis da Argentina e do Uruguai receberam, respectivamente, em 21 de agosto de 2012 e 30 de junho de 2014, da União Européia, o status de países com proteção de dados adequada, motivo pelo qual será feito o estudo comparado dessas legislações.

[2] Atualmente este Bloco Econômico conta com 05 (cinco) membros efetivos, os quatro membros originais da época da sua fundação (Brasil, Argentina, Uruguai, Paraguai) e a Venezuela, que ingressou no bloco posteriormente, aos quais se agregaram 03 (três) países associados (Bolívia, Chile e Equador).

Portanto, é possível delimitar a temática desta dissertação de forma que pretende discorrer sobre o tratamento jurídico dos dados pessoais na legislação de dois dos países do Mercosul que são considerados como garantidores de uma proteção adequada de dados pessoais, contrastando esse tratamento com as previsões recentemente incorporadas no ordenamento jurídico brasileiro a partir do Marco Civil da Internet.

E, por fim, considerando que dentre os 06 (seis) maiores provedores de acesso à *Internet* no Brasil, segundo a Pesquisa TIC Provedores de 2011, que detém em conjunto 78% (setenta e oito por cento) das conexões (CETIC.BR, 2011, p. 28), o provedor de acesso "Terra" é o único que tem expressiva atuação nos três países que serão analisados – Brasil, Argentina e Uruguai, o que suscita o seguinte problema de pesquisa: Tendo como base o nível de proteção já alcançado por dois dos quatro parceiros do Mercosul, é possível afirmar que as previsões do Marco Civil da Internet, bem como o que está previsto na minuta do Projeto de Proteção de Dados Pessoais, é suficiente e compatível com o nível já obtido nos demais Estados mercosulinos?

De outro lado, e tomando em consideração a implementação da legislação já existente nos demais Estados do Mercosul, é possível afirmar que a existência de normatização ampliou a proteção dos dados pessoais dos internautas, resultando em termos de políticas de privacidade mais protetivos em um dos maiores provedores de acesso que atua diretamente no Brasil e indiretamente nestes países – Terra, de forma a coibir a prática de segmentação comportamental por bancos de dados?

Portanto, o objetivo central desta dissertação é investigar o tratamento jurídico de dados pessoais nos Estados do Mercosul em face da segmentação comportamental utilizada pelas empresas que atuam no ambiente virtual. E, especificamente, com base nos termos de política de privacidade, constatar se a existência de legislação sobre o tema da proteção de dados surte efeitos positivos no sentido de proteger os dados pessoais do cidadão internauta.

Para tanto, são objetivos parciais desta pesquisa, realizar, inicialmente, um estudo teórico sobre o tema da segmentação comportamental que pretende identificar quais são os principais motivadores de tal prática, com base em categorias conceituais provenientes da Psicologia, da Publicidade e Propaganda e da Comunicação Social.

Ainda, analisar o tratamento jurídico destinado aos dados pessoais nos países integrantes do Mercosul, que receberam o título de países com uma proteção de dados adequada – Argentina e Uruguai, reconhecendo a sua proteção como uma nova categoria de direito fundamental, que foi, por sua vez, a questão de princípio essencial da presente dissertação.

Por outro lado, comparar as legislações da Argentina e do Uruguai e as previsões da Lei nº 12.965 de 23 de Abril de 2014 (Marco Civil da *Internet*), a fim de verificar se o nível de proteção de dados pessoais, recentemente conferido ao tema no Brasil, é adequado e suficiente para proteger os internautas em face da segmentação comportamental realizada na *Internet*.

Por fim, verificar como ocorre a proteção de dados pessoais do usuário por um dos principais provedores de acesso à *Internet* no Brasil, que também atua nos demais países comparativamente analisados, com base nas previsões dos termos de políticas de privacidade deste provedor de acesso nestes países.

A presente dissertação adotou uma abordagem dedutiva, portanto, sua elaboração partiu das novas estratégias empresariais empregadas na sociedade informacional, destacando a vulnerabilidade de dados pessoais ocorridas a partir dessas práticas. Uma vez assentadas as bases conceituais, avançando para o objeto específico, esta dissertação investigou as legislações de países do Mercosul que detém o selo de proteção de dados adequada concedido pela União Europeia, contrastando seus termos com as disposições da Lei nº 12.965, de 23 de Abril de 2014 (Marco Civil da *Internet*). Por fim e visando promover a aproximação entre o campo teórico e normativo com a realidade, realizou-se o estudo dos termos de políticas de privacidade do principal provedor de acesso à *Internet* que atua nestes países (Terra) especificamente no que tange à segmentação comportamental.

Concomitante à abordagem de feição dedutiva, foi utilizado o método de procedimento comparativo, empregado para aferir o grau de proteção entre as leis já existentes, bem como contrapô-las com a legislação que visa regulamentar parcialmente a matéria no Brasil, a Lei nº 12.965 de 23 de Abril de 2014 (Marco Civil da *Internet*) e o projeto de lei específico que pretendia tratar estritamente desta temática, arquivado no final do mês de janeiro de 2015. Também se recorreu ao método comparativo para realizar a análise das previsões dos diferentes termos de privacidade do referido provedor de acesso à *Internet*.

Aliado a esse método de procedimento, foi realizada pesquisa de natureza monográfica, empregada para a identificação e análise do fenômeno da segmentação comportamental no ambiente virtual, o que se concretizará especialmente pela análise dos termos de privacidade selecionados.

Inicialmente, foi utilizada a técnica de pesquisa bibliográfica em livros, periódicos, dissertações e teses, sobre o tema da proteção de dados pessoais, além de estudo na literatura acadêmica da Psicologia/Comunicação Social/marketing sobre a questão da segmentação comportamental. E, em um segundo momento, foi utilizada a técnica de pesquisa documental,

onde investigou-se as legislações da Argentina, do Uruguai e do Brasil e os termos de política de privacidade do portal e provedor de acesso "Terra" nestes países.

O presente trabalho adotou como marco teórico a obra do professor Antonio-Enrique Pérez Luño denominada "Derechos humanos, estado de Derecho y Constitución", elegida como forma decompreender uma estrutura de direitos humanos instituídosdentro de um estado de Direito e que é confrontada com os problemas derivados da sociedade informacional.

Tal escolha justifica-se pela importância do autor no que tange ao tema dos direitos humanos em face das relações com as TIC, já que defende um arcabouço mínimo de direitos ao cidadão internauta, algo que se alia aos objetivos desta dissertação. A essas justificativas, soma-se o fato de este autor estar inserido dentro uma tradição constitucional, que se assemelha à tradição constitucional brasileira e dos países que serão comparativamente analisados, o que permite um olhar sobre a questão da proteção de dados a partir de um paradigma constitucional dirigente e garantista.

Este marco teórico ainda foi composto pelas contribuições de Stéfano Rodotá em sua obra "A vida na sociedade da Vigilância – a privacidade hoje", pois é a partir da perspectiva da vigilância constante que se analisou a segmentação comportamental. Tal opção de marco teórico justifica-se por ser um autor que apresenta uma visão da atual sociedade, e, sobretudo, do valor privacidade, cuja análise perpassa por questões sociais, políticas e comunicacionais, as quais são imprescindíveis para o enfrentamento dos problemas envolvendo a violação de dados pessoais.

A importância social desta dissertação revela-se na essencialidade que atualmente o acesso à *Internet* tem na convivência dos indivíduos, produzindo reflexos nos mais variados segmentos de suas vidas, o que importa também na necessidade de identificar os riscos existentes aos seus direitos fundamentais, quando deste acesso. Da mesma forma, trata dos mecanismos de prevenção e promoção que são desejáveis, sobretudo diante da prática de segmentação comportamental através de bancos de dados pessoais digitais. Aliado a isso, destaque-se sua notável importância política, visto que pretende traçar comparativamente o perfil de como ocorre a proteção jurídica de dados pessoais nos países membros do Mercosul que já obtiveram o grau de países com proteção de dados pessoais adequada, concedida pela União Europeia, e, assim, refletir sobre eventuais formas de harmonização desses mecanismos, o que possibilitaria um mínimo de proteção jurídica aos internautas.

Esta dissertação trata de um tema juridicamente relevante que envolve a rede mundial de computadores (*Internet*) e, deste modo, insere-se na linha de pesquisa "Direitos da sociedade em Rede" da área de concentração "Direitos Emergentes da sociedade Global" do

Programa de Pós-Graduação em Direito (PPGD) (Mestrado em Direito) da Universidade Federal de Santa Maria (UFSM), pretendendo lançar um olhar humanizador para o uso das TIC, de maneira a aliar o desenvolvimento tecnológico com o respeito aos direitos e à dignidade dos internautas.

A organização dos capítulos foi pensada de forma a possibilitar ao leitor evoluir no entendimento do tema, compreendendo quais as categorias conceituais anteriores são essenciais para o entendimento das posteriores. Senão vejamos:

No primeiro capítulo, o grande objetivo é possibilitar a compreensão do fenômeno da segmentação comportamental por meio dos bancos de dados pessoais digitais e, para cumprir este desiderato, inicialmente haverá um estudo dos cenários onde esta forma específica de segmentação ocorre.

Estes cenários partirão de três premissas essenciais:

A primeira é que a sociedade capitalista foi profundamente alterada por uma revolução tecnológica ocorrida na década de 1970. A segunda é que o princípio constitucional de proteção da privacidade merece que sejam repensados os seus instrumentos jurídicos de proteção dentro desta nova realidade tecnológica, como um direito à proteção de dado pessoal autônomo à noção clássica de intimidade e vida privada. E, por fim, a terceira premissa é que as estruturas de vigilância e controle também foram potencializadas por esta realidade informacional.

Ainda, dentro deste primeiro capítulo, é essencial compreender os estudos sob o ponto de vista publicitário, psicológico e técnico que motivaram esta segmentação.

No segundo capítulo, dividido em três pontos, inicialmente a perspectiva da boa-fé objetiva – confiança e lealdade – será estudada como limitador teórico para evitar a utilização ilícita dos dados pessoais. Após haverá um estudo comparado entre as legislações da Argentina, do Uruguai e do Brasil, como forma de constatar o nível de proteção e a sua real capacidade de evitar a segmentação comportamental tratada no capítulo anterior.

Por fim, neste segundo capítulo, será feita a análise dos termos de política de privacidade do provedor de acesso “Terra” e como ele está disponibilizado nos três países cujas legislações foram analisadas no subcapítulo anterior. Esta segunda comparação visa constatar se o grau de proteção daquelas normas surtiu efeitos práticos sobre estes termos, tornando-os mais protetivos, com a finalidade de evitar a segmentação comportamental por bancos de dados pessoais digitais.

1 A SEGMENTAÇÃO COMPORTAMENTAL ATRAVÉS DO ACESSO A DADOS PESSOAIS NA *INTERNET*

O presente capítulo terá o objetivo de analisar os cenários sociais e jurídicos onde se desenvolveu a segmentação comportamental, com base em bancos de dados pessoais digitais, que deve ser entendida como o grande objeto de pesquisa do presente trabalho.

Como forma de cumprir esse objetivo, será essencial recorrer a teorias e categorias conceituais que não necessariamente foram feitas para utilização na área jurídica, porém, tendo em conta a necessária interdisciplinaridade que toda e qualquer pesquisa pensada dentro da área de concentração Direitos da Sociedade Global deve ter, acredita-se que este desafio é uma exigência.

Em um primeiro momento, serão traçados os cenários onde se situa a segmentação comportamental feita com base em bancos de dados pessoais, sendo utilizadas as noções da comunicação social e das ciências sociais essenciais para esta analise.

Esses cenários serão construídos com base em três realidades distintas. A primeira delas é a chamada Revolução Informacional – ocorrida na década de 1970 com o desenvolvimento e a utilização massiva das Tecnologias da Informação e da Comunicação (TIC) – e da sociedade informacional que ela acabou originando.

A segunda realidade é o aprofundamento que o princípio da proteção à privacidade sofreu no último quarto de século, passando a exigir o desenvolvimento de um novo direito dele decorrente, qual seja, a proteção de dados pessoais.

Por fim, a terceira será a busca por vigilância e controle, algo que sempre esteve presente na atuação estatal, mas que atualmente passou a ocorrer também nas relações entre entes não estatais – empresas da área tecnológica, sendo potencializado pela utilização das tecnologias informacionais.

Após a compreensão destes cenários, adentrando em um segundo momento do presente capítulo, será feito um estudo do objeto da pesquisa em si, isto é, da segmentação comportamental com base em bancos de dados pessoais digitais.

Inicialmente serão estudadas as motivações publicitárias que as empresas que praticam estas segmentações recebem das teorias contemporâneas do chamado Marketing de Relacionamento.

Ainda, para uma compreensão precisa de tal fenômeno, haverá um estudo da tendência, dentro da Psicologia contemporânea, que justifica e explica os efeitos que esta segmentação tem sobre os indivíduos a ela submetidos.

Por fim, encerrando este segundo momento, haverá um estudo dos bancos de dados pessoais digitais, que são tecnicamente responsáveis por fundamentar a segmentação comportamental, objeto desta pesquisa.

1.1 AS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO (TIC) E A AMPLIAÇÃO DA VIGILÂNCIA E DO CONTROLE.

As tecnologias, historicamente, surgiram como forma de solucionar as necessidades criadas pela sociedade. Porém, depois de desenvolvidas, muitas delas acabaram por modificar ealterar as relações interpessoais entre os indivíduos.

Com as Tecnologias da Informação e da Comunicação (TIC), tais como os computadores e a rede mundial (*Internet*), que surgiram a partir da década de 70 do século passado, não foi diferente. Elas trouxeram diversas vantagens aos indivíduos em suas relações na vida moderna, maior conforto e comodidade, velocidade nos processos de tomada de decisão,acesso a um grande volume de informações, nos mais diversos lugares.

No entanto, as TIC também trouxeram novos riscos e problemas à sociedade, como maior grau de isolamento físico entre os indivíduos, falta de organização das informações disponibilizadas, e, sobretudo, uma aceleração que provoca muitas vezes decisões precipitadas[3].

Um dos maiores riscos que a evolução tecnológica potencializou foi à vulnerabilidade dos direitos fundamentais, dentre eles a violação daquilo que classicamente se denominou privacidade, por meio de uma política institucional de controle e vigilância cada vez maior, especialmente em face de uma realidade que vivencia ameaças como o crescimento da violência e do terrorismo.

Sempre houve um grande interesse dos Estados por informações que digam respeito aos seus cidadãos, seja no intuito de manter o poder político estabelecido em Estados não democráticos, seja com a finalidade de, com certo grau de previsibilidade, compreender como agem e pensam os legítimos detentores do poder, em Estados Democráticos, ou seja, o povo.

Antes do avanço das TIC, a vigilância e o controle estatal encontravam muitas dificuldades práticas, sobretudo em populações grandes e diversificadas, o que acabava, de certa forma, minorando o grau de vulnerabilidade dos direitos fundamentais individuais dos cidadãos, que eram objeto deste processo.

[3]Tal visão negativa do avanço das TIC é defendia por autores como Ulrich Beck, em sua obra a "sociedade de risco- rumo à outra modernidade" e Paul Virilio na obra "Bomba informática".

Atualmente estas tecnologias permitem não só a captação, mas o armazenamento, o tratamento e o compartilhamento entre órgãos das informações pessoais de um grande número de indivíduos de forma praticamente instantânea, o que dificulta a proteção dos direitos desta população, dentre eles o direito à privacidade.

Considerando que o avanço das TIC geralmente surge a partir do investimento de empresas privadas, e tendo em conta que essas atualmente são as maiores prestadoras de serviços aos estados, o maior risco de violação dos direitos fundamentais, tais como a proteção de dados pessoais, encontra-se na atuação das grandes empresas do setor tecnológico.

A idéia de proteção à privacidade como um princípio constitucional fundamental exigiu uma reformulação dos seus mecanismos de proteção, inicialmente nos ordenamentos comunitários e nacionais dos países da União Europeia e após nos ordenamentos nacionais de diversos outros países (DONEDA, 2006), dentre os quais aqueles que serão analisados no segundo capítulo.

A proteção da privacidade passou a ser caracterizada, para além de um mero direito à não intervenção na esfera íntima da personalidade, como o tradicional "direito de ser deixado só", também um direito de intervenção no tratamento dado, tanto a nível físico como digital, às informações de caráter pessoal (RODOTÀ, 2008).

Deste modo, a antiga noção de princípio da proteção à privacidade como um mero impedimento de violações indevidas, uma aplicação negativa, com o aprofundamento deste princípio decorrente do avanço das tecnologias informacionais, ganhou a sua autonomia como direito fundamental próprio, referindo-se à proteção de dados pessoais.

O presente capítulo trata do embate entre uma realidade que tende cada vez mais à vigilância e ao controle por entes públicos e privados, justificando-se sempre na necessidade de uma maior segurança, em face da defesa de um novo direito surgido da evolução do princípio da privacidade, o direito à proteção de dados pessoais.

1.1.1 Da revolução informacional à *Internet*: entendendo os novos cenários.

Tecnologia e humanidade retratam uma relação que se estende há muitos séculos e que gera muita teorização, ou seja, surgem novas teorias sobre essa relação e essas são superadas na mesma velocidade com que são desenvolvidas as TIC.

Todavia, há algo em comum em todas essas teorizações[4], as tecnologias são desenvolvidas pelo homem – imerso em uma sociedade –, mas também ocasionam o desenvolvimento desse homem e, portanto, dessa sociedade.

No momento em que a primeira pedra foi entalhada até ganhar um formato circular e foi utilizada como forma de facilitar a tração e o transporte, os indivíduos que obtiveram essa tecnologia passaram a sofrer alterações em suas noções de espaço – que passou a ser percorrido com maior facilidade – e de tempo – pois esse espaço passou a ser percorrido em menor tempo, o que influenciou as suas relações interpessoais.

Portanto, a evolução da sociedade a partir de avanços tecnológicos não é privilegio da atualidade, uma vez que a história da humanidade experimentou importantes mudanças devido a descobertas que permitiram o desenvolvimento da civilização, dentre elas a escrita, que propiciou às pessoas evoluir da comunicação oral a uma comunicação gráfica. (LIMBERGER, 2007, p. 51).

Evoluções sociais decorrentes de avanços tecnológicos não constituem uma exclusividade do tempo atual. Além da escrita, a máquina à vapor ou à eletricidade, quando do seu surgimento, também impulsionaram diversas alterações na sociedade.

Sem adentrar em abordagens ingênuas e simplistas sobre o poder do desenvolvimento tecnológico, é uma obviedade que, ao longo do processo evolutivo da humanidade, o desenvolvimento científico foi uma resposta histórica a problemas sucessivos de cada época e contexto histórico.

Deste modo a tecnologia corrente não é mais que o esforço da ciência para responder, nem sempre de forma adequada, às questões levantadas por novas formas de convivência e à expansão implacável das aspirações e necessidades sociais (PEREZ LUÑO, 2014-A, p. 51).

Com as TIC, desenvolvidas na década de 70 do século XX, não foi diferente. Assim que passaram a tornar-se parte integrante da vida do homem, elas o desenvolveram de alguma

[4] Teorizações que tentam tratar do avanço das tecnologias e da sua vinculação com as relações interpessoais dos indivíduos, ora visualizando que elas trazem inúmeras vantagens a estas relações, são os chamados ciberotimistas, dos quais o maior defensor é Pierre Lévy (2005); ora visualizando os inúmeros riscos e problemas que elas causam, neste caso os chamados ciberpessimistas, como Paul Virilio (1999).

forma, pois ele passou a exercer suas atividades com maior conforto e comodidade, detendo um grau de informação maior. No entanto passou a estar sujeito a uma nova gama de riscos antes desconhecidos.

No final do século XIX e o início do século XX, as utopias positivas deram lugar às negativas. As utopias ‘de desejo’ foram substituídas por aquelas ‘de angústia’ (RODOTÁ, 2008). Porém a angústia do futuro não implica na sua recusa, visto que ao lado da percepção, cada vez maior, dos riscos do progresso tecnológico, está a consciência da impossibilidade de deter tal progresso.

Desta forma, para Stéfano Rodotá (2008, p. 41):

> A ruína da ideia de um progresso sempre e, de qualquer forma, positivo, chama a atenção para o fato de que o mundo pode ser melhor somente se os homens o quiserem. Dessa consciência nasce à imagem que acompanhará habitualmente, daqui por diante, os discursos sobre os efeitos sociais das tecnologias: a do deus bifronte, Janos.

O avanço da Informática, nas últimas décadas do século passado, não significou simplesmente uma evolução social, mas sim a transformação nos mais diversos níveis de sociabilidade, dentre os quais as relações familiares, comunitárias, profissionais e, por que não, políticas.

Neste período, inúmeros

> acontecimentos de importância histórica ímpar transformaram o cenário social da vida humana, dentre eles uma revolução tecnológica concentrada nas tecnologias da informação e da comunicação começou a remodelar a base da sociedade em ritmo extremamente acelerado. (CASTELLS, 2003-A, p. 39).

Quando se utiliza o termo tecnologias informacionais, o que se está a tratar é dos chamados instrumentos que utilizam a informação como forma de manejo e obtenção de mais informação.

Esta categoria conceitual – sociedade informacional – não tem qualquer condão de limitar a compreensão; o seu grande objetivo é exatamente o contrário, isto é, ampliar a percepção das relações que são alteradas por essas TIC.

Como esclarece Armand Mattelart (2002, p. 11)

> A idéia de uma sociedade regida pela informação, está, por assim dizer, inscrita no código genético do projeto de sociedade inspirado pela mística do número. [...] O pensamento do enumerável e do mensurável torna-se protótipo de todo o discurso verdadeiro ao mesmo tempo em que instaura o horizonte da busca da perfectibilidade das relações humanas.

Segundo Castells (2003-A, p. 51), a denominada "sociedade informacional"[5] pode ser caracterizada como o surgimento de uma estrutura social associada a um novo modo de desenvolvimento, o informacionalismo, historicamente moldado pela reestruturação do modo capitalista de produção.

Nesse modo de desenvolvimento, visualiza-se a ação de conhecimentos sobre os próprios conhecimentos como principal fonte de produtividade, pois o processamento da informação é focalizado na melhoria da tecnologia deste próprio processamentocomo fonte de produtividade, em um círculo virtuoso entre as fontes de conhecimento tecnológico e a aplicação destas para melhorar a geração de conhecimento e o processamento da informação.

A relação entre a cultura de uma sociedade e o seu meio de desenvolvimento ocorre na medida em que este molda as relações comunicacionais, que se constituem em um importante substrato da cultura vigente. E como o informacionalismo baseia-se na tecnologia de conhecimento e informação, há uma íntima ligação entre cultura e as forças produtivas, e entre o espírito e a matéria, no modo de desenvolvimento do informacionalismo.

A industrialização permite que a técnica e a organização rimem (MATTELART, 2002, p. 33), sendo possível identificar um fio de condução entre a noção de divisão do trabalho teorizada pela economia política, a divisão das operações mentais que estão na base da mecanização do pensamento e a doutrina da gestão científica da oficina. E, assim, as utopias da comunidade universal e da sociedade descentralizada pontuam o avanço das redes de comunicação.

Como pressuposto básico para compreensão do fenômeno informacional, tem-se a visão sistêmica de que não é possível estudar o conjunto das relações sociais, econômicas, culturais, afetivas e políticas, transformadas pelas tecnologias separando-as, mas sim a partir de sua interação.

Economia, empresas, sociedade e cultura são diferentes elementos de um mesmo sistema interligado e, dessa forma, uma totalidade integrada de partes diferenciadas formando um todo organizado que propicia a consecução de algum fim a partir de suas interações conjuntas.

O avanço de um capitalismo de mercado, causa deste imenso avanço tecnológico, traz uma grande preocupação no sentido da transformação da personalidade humana e,

[5] Importante realizar uma distinção conceitual que o próprio Castells (2003-A, p. 64-5) faz, ele diferencia "sociedade informacional" de "sociedade da Informação", sendo aquela uma sociedade moldada pelas TIC Informacionais e Comunicacionais que surgiram da chamada 3ª Revolução Industrial, historicamente localizada na década de 70 do século passado, enquanto que esta se caracteriza como toda a sociedade, mesmo antes do desenvolvimento das TIC na década de 70, onde a informação ganhou um papel primordial.

consequentemente, dos dados que expressam esta personalidade em um produto ou fator de produção, como expõe Jeremy Rifkin (2005, p. 09):

> Estamos viajando para um novo período em que um número crescente de experiências humanas é comprado na forma de acesso a redes multifacetadas no ciberespaço. Essas redes eletrônicas dentro das quais um número crescente de pessoas gasta grande parte de seu dia-a-dia, são controladas por algumas poderosas empresas transnacionais da mídia que possuem as linhas de comunicação entre elas e que controlam grande parte do conteúdo cultural que compõe as experiências pagas em um mundo pós-moderno.

Assim, chega-se à denominada "era do acesso", que pode ser bem definida pela "crescente transformação em *commodity* de toda a experiência humana. Redes comerciais de todos os tipos e formas navegam pela Web em torno da totalidade da vida humana, reduzindo todo o momento de experiência vivida em status" (RIFKIN, 2005, p. 79).

Nesta "era do acesso", as novas formas de coleta e tratamento de informações pessoais (RODOTÁ, 2008, p. 24), possibilitadas, sobretudo, pelo recurso a computadores, adicionam-se à crescente necessidade de dados por parte das instituições públicas e privadas.

Não é possível imaginar uma ação que vá de encontro a esta tendência, comum a grande maioria das organizações sociais. É preciso considerar como ocorre tal situação, e, acima de tudo, analisar as transformações que ela causa na distribuição e no uso do poder por estas estruturas.

Portanto, a imensa necessidade de dados pelas instituições acaba transformando a estrutura destas, como forma de possibilitar a obtenção de um número maior destas informações, interligando diferentes setores e transferindo-as a uma velocidade cada vez maior entre eles.

Como afirma Armand Mattelart (2002, p. 81), "a futurologia técnica planta o cenário que preside a construção das idéias encarregadas de anunciar, se não de explicar, que a humanidade está no limiar de uma nova era da informação e, portanto, de um novo universalismo".

Afinal, qual foi o grande momento de ruptura em que é possível identificar o surgimento da sociedade informacional? E quando se iniciou esta nova era?

Como já dito, ela surgiu em meados da década de 70, início da década de 80, na Califórnia, nos Estados Unidos da América, mais precisamente na região atualmente conhecida como Vale do Silício, onde ocorreu a Revolução Informacional. (CASTELLS, 2003-A, p. 39)

Neste local, uma nova geração de cientistas e engenheiros passou a trabalhar em projetos de máquinas movidas a mecanismos chamados "processadores de informação", os

denominados “computadores”, e em redes de comunicação entre estas máquinas, inicialmente limitadas a poucos pontos de conexão e posteriormente pensadas de forma global, como a *Internet* (CASTELLS, 2003-A).

Em um primeiro momento, estes projetos obtiveram apoio financeiro e político do exército americano, pois estas máquinas e, principalmente, suas redes de conexão eram consideradas um mecanismo de defesa extremamente interessante. Este interesse militar era justificado pelo fato de que as TIC adotavam uma lógica de descentralização da informação e da comunicação, o que poderia, na eventualidade de um ataque de um inimigo estrangeiro, reorganizar as defesas do país a tempo de um contra-ataque. (CASTELLS, 2003-C, p. 13)

Após o financiamento militar, as universidades e instituições de ensino da época viram no desenvolvimento de computadores e redes de conexão uma forma de facilitar a comunicação e a troca de experiências, algo essencial a qualquer pesquisa científica. Com o envolvimento das Instituições de Ensino, muitos jovens, estudantes universitários – que na época estavam fortemente influenciados pela cultura comunitária *hippie* dos *campi* universitários – passaram a dedicar o seu tempo a projetos que envolviam TIC, alterando o perfil dos responsáveis pelo desenvolvimento e aprimoramento destes mecanismos, o que fez com que estas tecnologias, além de informacionais, passassem a ser altamente comunicacionais (LÉVY, 2004, p. 32).

Deste modo essas tecnologias se desenvolveram “num ambiente seguro, propiciado por recursos públicos e pesquisa orientada para uma missão, mas que não sufocava a liberdade de pensamento e inovação” (CASTELLS, 2003-C, p. 24)

Após ser direcionada e influenciada pela cultura militar e pelas noções científicas provenientes das Instituições de Ensino, a Revolução Informacional foi fortemente influenciada pelo sistema capitalista, pois a utilização massiva de tecnologias e redes de comunicação passou a ser considerado um negócio altamente rentável.

Assim, compreendido que o informacionalismo é um modo de desenvolvimento de um determinado modo de produção – capitalismo, pode-se afirmar que ele está ligado à expansão e ao rejuvenescimento deste, como o industrialismo esteve ligado a sua constituição como modo de produção.

As condições de espaço e tempo da Revolução Informacional influenciaramo desenvolvimento da sociedade que a partir dela se estabeleceu, seja pela noção libertária da sociedade americana, espaço onde iniciou essa revolução, seja pelo incessante ambiente de disputa ocasionado pela Guerra Fria, período de tempo onde ela se desenvolveu.

Portanto, entende-se que a sociedade informacional adotou a forma econômica do local onde surgiu – capitalismo americano – o que, por sua vez, alterou significativamente a estrutura das empresas e, consequentemente, a forma das relações de trabalho, que ocasionaram uma modificação cultural da sociedade e, devido a isso, surgiram novas formas de relações interpessoais entre os sujeitos.

Em face das enormes e ainda inexploradas possibilidades que a nova tecnologia oferece – a sua candidatura a único meio que permitirá dominar as infinitas variáveis de uma organização social cada vez mais condicionada pelo crescimento das necessidades e a escassez de recursos –, estão os riscos ligados a um avanço impetuoso que a programação política e institucional até agora não foi capaz de acompanhar (RODOTÁ, 2008, p. 38).

Com o avanço das novas TIC o aumento das possibilidades sociais de criação de riquezas potencializa o surgimento de novos riscos sociais, equivalentes às possibilidades positivas deste avanço, como afirma Urlich Beck (2010, p. 23): "Consequentemente, aos problemas e conflitos distributivos da sociedade da escassez sobrepõem-se os problemas e conflitos surgidos a partir da produção, definição e distribuição de riscos científico-tecnologicamente produzidos."

Tendo em conta que culturas são basicamente formas de comunicação, surge, para Pierre Lévy (2005, p. 273), uma nova estrutura cultural denominada "virtualidade real", onde não há separação clara entre a realidade – entendida como mundo físico – e as representações simbólicas – entendida como o mundo virtual.

Para uma compreensão deste cenário onde se estabeleceu a Revolução Informacional, é importante identificar a denominada cultura "universal sem totalidade"[6].

Esta visão de universal sem totalidade é importante para a compreensão do fenômeno informacional, pois assim como as tecnologias surgidas neste período buscavam ter um alcance global, elas tentavam auxiliar o seu próprio desenvolvimento, sendo autorreflexivas.

E a importância da compreensão deste cenário justifica-se pela questão de que nunca antes na história da humanidade (CASTELLS, 2003-A) tecnologias foram desenvolvidas de uma forma massiva, não com o objetivo de utilização direta pelo homem, mas sim para o desenvolvimento de outras tecnologias.

---

[6] Nesta proposição, o universal significa a *presença virtual da humanidade em si própria*. O universal inclui o aqui e agora da espécie, o seu ponto de encontro, um aqui e agora paradoxal, sem lugar nem tempo claramente assinaláveis. O que é então totalidade? Trata-se da unidade estabilizada do sentido de uma diversidade. Que esta unidade ou esta identidade sejam orgânicas, dialéticas ou complexas mais do que simples ou mecânicas não altera nada: trata-se sempre de uma totalidade, isto é uma compartimentação semântica englobante. (LÉVY, 2005, p. 273-274)

Na questão dos dados, esta percepção é essencial, pois muitos sistemas surgiram não para facilitar ou trazer alguma comodidade ao gestor desses dados, mas sim para possibilitar o tratamento destas informações de forma automática. Além disto, estas TIC tentavam abarcar todo o acumulo cultural produzido pela humanidade até então na forma de informações e dados, ao mesmo tempo em que eram desenvolvidas dentro que uma perspectiva cultural altamente vinculada às circunstâncias de tempo e de espaço de seu desenvolvimento inicial.

Dentre as invenções surgidas durante a revolução informacional, está a rede mundial de computadores – *Internet* – que trouxe uma possibilidade de comunicação simultânea jamais presenciada pela humanidade.

A *Internet* é baseada em uma linguagem determinada em bits e, desta forma, duas consequências imediatas podem ser observadas, por Nicholas Negroponte (1995, p. 23):

> Em primeiro, os bits misturam-se sem qualquer esforço. Começam a mesclar-se e podem ser utilizados e reutilizados em seu conjunto ou separadamente. Em segundo lugar, nasce um novo tipo de bit – um bit que conta sobre outros bits (informação para organização de informação).

Inicialmente a *Internet* prenunciava uma nova era, onde a liberdade de expressão poderia se difundir através do planeta sem depender da mídia de massa, uma vez que muitas pessoas podiam interagir com outras tantas de maneira irrestrita.

Da mesma forma, a privacidade era protegida pelo anonimato da comunicação e pela dificuldade de investigar as origens e identificar o conteúdo de mensagens transmitidas com o uso de protocolos da *Internet*.

O fenômeno da informática (PEREZ LUÑO, 2005, p. 343) possibilitou uma verdadeira revolução no âmbito dos métodos tradicionais para a organização, registro e utilização das informações. A dimensão quantitativa das informações que podem ser armazenadas e transmitidas é de tal magnitude que chegou a um patamar que obriga relacionar os problemas entre a privacidade e a informática a partir de um novo prisma, isto é, as questões jurídicas e políticas devem ser respondidas de forma a respeitar a realidade do trânsito dessa quantidade de informações, reconstruindo direitos e conceitos.

Os já afirmados fundamentos de liberdade na *Internet* também têm sido desafiados pelas TIC e regulações, visto que a aplicação de software pode ser sobreposta em camadas

nos protocolos da *Internet*[7], tornando possível identificar rotas de comunicação e conteúdo, controlando e vigiando o que os indivíduos acessam e afirmam na rede.

Essa nova tecnologia comporta a atuação de novos atores que irão intermediar dos computadores dos indivíduos, visto que ela pode ser compreendida como uma "rede internacional de computadores conectados entre si. É hoje um meio de comunicação que possibilita o intercâmbio de informações de toda a natureza, em escala global, com um nível de interatividade jamais visto anteriormente" (LEONARDI, 2005, P. 1).

Inicialmente a Agência Nacional de telecomunicações (ANATEL) estabeleceu no item 3 a alínea "a" da Nota Técnica nº 004 de 1995, que a *Internet* é um "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "software" e os dados contidos nestes computadores" (ANATEL, 2014)

Atualmente no Brasil, o conceito de *Internet* tem previsão na Lei do Marco Civil da *Internet* (comentada no capítulo anterior) que, em seu artigo 5º, estabelece ser a *Internet*: "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes" (BRASIL, 2014)

Mas como funciona esta rede? Isto é, qual é a lógica de funcionamento desta tecnologia?

A *Internet* funciona a partir da conexão entre computadores que, esquematicamente, formam uma grande árvore, onde os maiores galhos são as espinhas dorsais do sistema, denominado *backbones*, estruturas constituídas de roteadores de tráfico interligados por circuitos de alta velocidade. Estas estruturas são capazes de manipular grandes quantidades de informações. Para a conexão com estas estruturas é essencial os serviços de provedores de informações ou de acesso, que serão responsáveis pela conexão do usuário com o sistema.

Cada um dos computadores que está vinculado à *Internet* é parte de uma rede própria, que se agrega a uma malha de um provedor de acesso – que tem o seu próprio servidor – e que, por sua vez, une-se a um *backbone*, responsável por possibilitar a conexão e a troca de informações entre os demais servidores de acesso e, consequentemente, entre os computadores a eles interligados. Todo este sistema é intermediado por empresas prestadoras

[7] A *Internet* funciona através de camadas de códigos que podem ser sobrepostos por outros códigos, que significam termos ou nomes específicos, que passam a filtrar a informação que transita na rede e dessa forma localizar os indivíduos que tenham referido tais termos (CASTELLS, 2003-C, p. 140).

de serviço, que possibilitam tanto a conexão do usuário final – provedores de acesso – quanto o funcionamento dos provedores – provedores de *backbone*.

Estas empresas, independentemente de sua espécie, de provedores de acesso ou de *backbone* – em determinado locais chamados de pontos de presença (POP[8]), são os locais onde estão os equipamentos, grandes computadores servidores, que possibilitam a conexão de múltiplos usuários a rede.

Na realidade não há um centro ou um ponto de presença central que controle e determine a conexão de todos os servidores, isso seria ilógico, considerando que a *Internet*, assim como uma rede, foi pensada em uma arquitetura não hierárquica ou centralizadora, não se caracterizando como um mero sistema linear de comunicação. Portanto, não existe uma rede de *Internet*, mas sim diversas teias que se conectam entre si através dos chamados pontos de acesso (NAPs[9]), que têm a função primordial de possibilitar a conexão de computadores que não estão integrados na mesma rede (CARVALHO, 2001, p. 160).

Os diferentes provedores precisam de diversos POPs localizados nas principais regiões do país, locais onde há uma grande quantidade de computadores com uma alta capacidade de processamento, que são responsáveis pelas conexões dos usuários daquelas localidades.

Na realidade os provedores de *backbone* têm o papel fundamental de possibilitar tecnicamente a conexão entre computadores, seja pela estrutura de cabos de fibra ótica ou pelos supercomputadores que possuem a conexão entre diferentes provedores de acesso (VOGAS, NEUMARY, 2009, p. 3966).

Na rede mundial de computadores, centenas de provedores são conectados a pontos de acesso à rede em diversas cidades, com enorme quantidade de dados trafegando entre as redes em tais pontos. Assim a *Internet* "representa um grande conjunto de redes de computador, as quais se comunicam por intermédio de pontos de acesso, permitindo assim que cada computador na rede se conecte a qualquer outro." (LEONARDI, 2005, p. 6)

Além dos *backbones*, que servem como estruturas de conexão, para o controle do tráfego de informações entre diferentes computadores são necessárias estruturas denominadas roteadores, que determinam para onde as informações devem ser enviadas e de que forma isto será feito (TELLINI, 2006, p. 62).

Basicamente os roteadores exercem duas importantes funções: inicialmente asseguram que determinas informações cheguem ao destino que se objetiva e, em segundo lugar,

[8] Sigla decorrente da expressão em inglês *point of presence*.
[9] Sigla decorrente da expressão em inglês *network access point*.

impedem que estas informações trafeguem onde não devam, e, portanto que outros dados desnecessários atrapalhem a conexão entre usuários.

Assim, a função básica do roteador é possibilitar o fluxo de dados entre diferentes redes de conexões, considerando que a *Internet* é um grande sistema que viabiliza a conexão de milhares de computadores e a transmissão das mais diversas espécies de informações entre eles.

Como qualquer forma de comunicação, mesmo aquelas de caráter interpessoal, estas conexões e transmissões de dados somente são possíveis se nos pólos deste processo comunicativo existam computadores que dialoguem a partir dos mesmos códigos comunicacionais.

A *Internet* tem sua linguagem universal, que possibilita a comunicação entre os mais diversos pontos do globo. Esta linguagem é denominada Protocolo de Controle e Transmissão/Protocolo de *Internet* (TCP/IP[10]), que funciona através da transmissão de pacotes de dados (VOGAS, NEUMARY, 2009, p. 3966).

De forma simples, o TCP divide as informações em pequenos pedaços, denominados pacotes, e após a transmissão, o mesmo TCP reúne novamente os pacotes de informações, formando o conteúdo inicial. Já o IP adiciona a cada pacote de dados o endereço do destinatário para que eles atinjam o alcance correto, independentemente da quantidade de roteadores e computadores que participem do processo. Assim, o IP funciona como o nome do destinatário em uma correspondência, impossibilita que a informação seja enviada a um endereço diferente. Em razão disso, mesmo que os diferentes pacotes de informações trafeguem por diferentes caminhos, chegam ao destino.

Como esclarece Marcel Leonardi (2005, p. 7):

> O protocolo TCP/IP divide os dados a serem transmitidos em pacotes de dados de tamanho variável. Cada pacote, portanto, além de parte dos dados transmitidos, carrega também as informações necessárias para chegar a seu destino, ou seja, o endereço de seu remetente, o endereço do seu destinatário, o número total de pacotes em que tal informação foi dividida, e o número daquele pacote específico.

Cada conjunto de informações é enviado ao destinatário pela melhor rota possível, a qual pode ou não ter sido utilizada pelos demais e, em razão disso, a *Internet* é eficiente e permite o acesso de milhões de usuários, pois o trafego de dados é balanceado entre as rotas

[10] Sigla decorrente da expressão em inglês *Transmission Control Protocol*/*Internet Protocol*.

possíveis, e eventualmente, caso alguma delas esteja impossibilitada, a linguagem do sistema localiza uma rota melhor e redireciona o trafego.

Como qualquer correspondência do mundo físico, cada pacote de dados precisa do endereço do seu remetente e do endereço do seu destinatário, que no caso serão os seus respectivos Ips. Assim toda a vez que um usuário acessa a uma determinada rede, seu computador recebe um número de IP que funcionará como o seu endereço de envio e de recepção dos pacotes de dados.

Antes da massificação da utilização da *Internet*, quando o sistema tinha uma lógica mais rudimentar, os usuários, para se comunicarem com determinados computadores, precisavam identificar os seus respectivos endereços de IP e decorar tais números, o que tornava o processo de conexão lento e pouco usual.

Porém, na década de 80, desenvolveu-se uma tecnologia que possibilitava a substituição dos endereços numéricos por textos, o chamado sistema nome de domínio (DNS[11]), que funcionava de forma a vincular determinado texto (domínio) aos respectivos endereços de IP. Assim bastava conectar-se a um servidor DNS, que ele iria localizar o respectivo protocolo de *Internet* do destinatário (TELLINI, 2006, p. 63).

Os servidores de DNS funcionam da seguinte forma: ao receber a informação do domínio, procuram localizar e reconhecer o número de IP equivalente àquela informação textual. Caso localizem, enviam o IP ao usuário, que pode conectar-se a este computador e receber as informações que precisa. Caso não localizem o IP, entram em contato com outros servidores DNS e questionam se eles têm registrado o numero de IP que se refere àquele domínio, e, se estes servidores também não localizam, enviam uma mensagem de erro ao usuário (KAZMIERCZAK, 2011, p. 469).

O sistema DNS funciona pela redundância, pois existem múltiplos servidores em cada ponto de transmissão, de forma que, se um deles desconhecer a informação ou falhar, outro poderá processar a requisição feita pelo usuário (TELLINI, 2006, p. 63).

Além disso, os servidores DNS têm outra importante função, o armazenamento temporário (ou *caching*), que simplesmente significa que o servidor arquiva as informações pesquisadas por determinado IP, tornando desnecessária a conexão com outros servidores, caso o usuário pretenda novamente acessar aquela informação, evitando assim uma sobrecarga do tráfego de dados na rede.

---

[11] Sigla decorrente da expressão em inglês *Domain Name System*

Todo este processo não é visível. É feito automaticamente, milhares de vezes por hora, por milhões de usuários que, em sua grande maioria, desconhecem este funcionamento, apenas buscam as informações a partir dos domínios que conhecem, sem se preocuparem com a forma como este acesso ocorre.

Os dados que trafegam na rede são armazenados por servidores, que na realidade são todos os computadores que se conectam à rede, assim, todos funcionam como servidores e, ao mesmo tempo, nenhum deles tem esta função específica, e por isso, em termos informáticos, são chamados de clientes (TELLINI, 2006, p. 62).

Quando o usuário acessa um site, seu computador funciona como um cliente, que obtém dados do servidor onde está localizado aquele *web site* – computadores cliente sempre acessam os servidores com objetivos determinados e, portanto sua solicitação é processada automaticamente por um programa específico criado para aquele serviço (TELLINI, 2006, p. 56).

Cada servidor disponibiliza portas de conexão para cada serviço que presta aos seus clientes. Estas portas de conexão são vias de acesso entre o servidor e os computadores cliente, portanto, cada computador cliente conecta-se a um servidor através de um endereço e IP específico e por intermédio de uma porta de conexão que se refere ao serviço que será prestado (KAZMIERCZAK, 2011, p. 469).

Assim torna-se possível que os dados sejam compartilhados de diversas formas, de acordo com o meio de transmissão utilizado. Dentre estas formas, o meio mais conhecido é a *world wide web*[12], a "teia de escala global", que permite aos usuários buscar e obter informações armazenadas em servidores de acesso remoto, bem como, em alguns casos, interagir com tais servidores.

Em termos concretos, a *web* consiste em um vasto numero de informações, documentos e dados armazenados em diferentes computadores ao redor do planeta. Para acessar a *web*, basta o indivíduo ter conhecimento do seu endereço e digitá-lo em um campo específico e, assim, poderá acessar o conteúdo que aquela página de *Internet* contém.

Na realidade a *web* funciona como uma grande biblioteca com uma gama praticamente infindável de informações sobre os mais diversos assuntos, e que estão disponibilizadas de forma rizomática, por meio de um sistema de *links*, variando-se o grau de acesso aos mais diferentes indivíduos.

[12] Ou simplesmente *Web*.

Todo este processo de funcionamento exige a execução de diversos serviços que são prestados por entes denominados provedores, mas precisamente, provedores de serviços de *Internet*.

Provedores de serviços de *Internet* caracterizam um gênero do qual são espécies os provedores de *backbone*, de acesso, de correio eletrônico, de hospedagem e de conteúdo. Basicamente esta distinção tende a perder a sua razão de existir em virtude de que, cada vez mais, os principais provedores de serviços de *Internet* acabam exercendo diferentes funções.

Como esclarece Marcel Leonardi (2005, p. 19), a razão desta perda de importância da diferenciação decorre do fato de que "a função dos provedores de acesso – disponibilizam conexão de seus usuários a *Internet* – evoluiu em razão do tempo e do crescimento da utilização da rede." Atualmente é comum que os provedores de acesso também ofereceram diferentes serviços aos seus clientes, tais como hospedagem de *web sites*, manutenção de contas de e-mail, conteúdo exclusivo, servidores para fins específicos, etc.

Os *backbones* representam o nível máximo na hierarquia técnica de uma rede de computadores, são na realidade estruturas físicas formadas por cabos de fibra ótica de alta velocidade, por onde trafegam a quase totalidade dos dados transmitidos através da *Internet* (VOGAS, NEUMARY, 2009, p. 3966).

Estes *backbones* são administrados por pessoas jurídicas que efetivamente detêm a propriedade da estrutura física capaz de manipular grandes volumes de dados, através de roteadores de tráfego interligados por circuitos de alta velocidade, e que disponibilizam, a título oneroso, tais estruturas aos provedores de acesso e de hospedagem.

Geralmente as conexões à *Internet* ocorrem através de provedores de *backbone* que não são de conhecimento do usuário final. Estas estruturas são negociadas com os provedores de acesso responsáveis por manter os usuários conectados ao sistema.

Conforme a Rede Nacional de Pesquisa (RNP), este provedor é uma "Entidade mantenedora de rede de longa distância (WAN), de âmbito multiregional ou nacional, com o objetivo básico de "repassar" conectividade à rede através de vários pontos de presença judiciosamente distribuídos pela região a ser coberta" (BRASIL, 2014-A, p. 7).

As pessoas físicas ou empresas obviamente podem conectar-se à *Internet* diretamente através dos provedores de *backbone*, porém, como os custos para este tipo de estrutura ultrapassam a casa dos milhões de reais, não é uma tecnologia utilizada de pela grande maioria da população.

Diante disso, o internauta comum precisa contar com um ente que intermedia esta relação entre a estrutura da *Internet*, contratando um provedor de *backbone* para que este acesso ocorra a um preço razoável.

O provedor de acesso é um "varejista" de conectividade à *Internet* e, como tal, opera em diversas escalas, possibilitando o acesso a um ou poucos computadores, até tornando possível a conexão de uma ampla rede formada por centenas de máquinas (CARVALHO, 2001, p. 158).

Estes provedores de acesso podem livremente estabelecer os preços pela intermediação desta conexão, e tal liberdade é fundamental para possibilitar que uma amplitude cada vez maior de sujeitos tenham acesso a tal serviço e, consequentemente, possam tornar-se usuários da *Internet*.

Esta diversidade no acesso decorre de uma realidade onde o uso de tais tecnologias varia entre os indivíduos. Alguns utilizam a rede como instrumento de trabalho, outros como forma de socializarem-se, outros como meio de entretenimento, enfim para as mais diversas finalidades. Todos têm o direito de que seja cobrado um preço justo, levando-se em consideração a utilização que dá para a *Internet*.

Portanto o papel primordial do provedor de acesso é possibilitar a conexão dos usuários à *Internet*, atribuindo a eles um endereço de IP, através do qual poderão receber os pacotes de dados referentes às informações que pretendem obter. Além disto, é responsável por direcionar o usuário a uma rede de cabos de fibra ótica (*backbone*) que vai possibilitar a transmissão e a recepção das informações que estes indivíduos desejam (CARVALHO, 2001, p. 168).

Realmente muitos provedores de acesso passam a prestar diversos outros serviços, porém o mais importante deles é possibilitar o acesso dos seus clientes à *Internet* e para tanto recolhem e transmitem informações dos usuários.

Essa forma de atuação explica como o uso destas tecnologias possibilita violações à privacidade, uma vez que se torna possível relacionar indivíduos com processos próprios de comunicação em contextos institucionais específicos. Assim, todas as formas tradicionais de controle político e organizacional podem ser lançadas sobre o indivíduo em rede (CASTELLS, 2003-C, p. 139-140).

Esta nova realidade determinada pelo uso de computadores no tratamento das informações pessoais torna cada vez mais difícil considerar o cidadão como um simples 'fornecedor de dados', sem que a ele caiba algum poder de controle.

As informações coletadas (RODOTÁ, 2008, p. 36-7) permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes e, consequentemente, os cidadãos passam a ter o direito de exercer controle direto sobre aqueles sujeitos aos quais as informações fornecidas atribuirão um crescente aumento de poder.

Uma das grandes características da nossa época, sem dúvida, é a progressiva publicização da vida. As sociedades atuais cada vez mais deixam menos resquícios para a existência privada solitária, subtraída da ingerência e da indiscrição do público.

Enfim, os sinais do tempo presente parecem destinados à exposição e a intensas visualizações, ao contrário do silêncio e da solidão das épocas anteriores. Se considerados aspectos qualitativos da vida, nestas condições o reduto do privado fica paulatinamente mais vulnerável e se obriga a repensar-se e tornar-se exíguo ante a invasão do público (PEREZ LUÑO, 2005, p. 351).

Como esclarece Kaminsk (2000, p. 100-101):

> A tecnologia não é neutra. É a junção entre ciência, mercado e sociedade. Mas a tecnologia, por si só, não viola a privacidade – e sim as pessoas que utilizam essa tecnologia, criada para suprir necessidades, e a política por detrás da tecnologia. Pode ser usada para invadir a privacidade, e pode ser usada para protegê-la. [...] Em suma, a tecnologia deve garantir aos indivíduos o direito à privacidade na *Internet*. E a privacidade das informações deve ser valorizada por todos aqueles que valorizam a liberdade. Devemos mudar nossa forma de pensar, nossas leis e nossa sociedade. Devemos criar um futuro que preze a liberdade, e que honre a autonomia e a privacidade pessoal. E devemos começar agora.

Com o surgimento da rede mundial de computadores (*Internet*), passou-se a identificar um espaço não local chamado de Ciberespaço[13].

Dentro deste Ciberespaço, o desenvolvimento e o emprego de tecnologias, seja no âmbito da natureza, da sociedade ou da personalidade, sobrepõe-se a questões políticas e científicas – administração, descoberta, integração, prevenção, acobertamento – dos riscos de tecnologias efetiva ou potencialmente empregáveis, tendo em vista "horizontes de relevância" (BECK, 2010, p. 24) a serem especificamente definidos.

Dessa forma, a promessa de segurança avança com os riscos e precisa ser, diante de uma esfera pública alerta e crítica, continuamente reforçada por meio de intervenções cosméticas[14] ou efetivas no desenvolvimento técnico-econômico (BECK, 2010, p. 24).

---

[13] Lévy (2005, p. 276) explica que o "Ciberespaço" significa para o homem "o pulular das suas comunidades, o emaranhado de suas obras, como se toda a memória dos homens se desdobrasse nesse instante: um imenso ato de inteligência coletiva sincronizando, convergindo para o presente, relâmpago silencioso, divergente convergindo como uma cabeleira de neurônios"

Diante destas intervenções,é plenamente possível propugnar a releitura dos direitos fundamentais (LIMBERGER, 2007, p. 35) com base nos valores superiores do ordenamento jurídico: a liberdade, a justiça, a igualdade e o pluralismo político, bem como a dignidade na perspectiva do fenômeno informático, e, dessa forma, a informática atuará a serviço do homem, e não como diminuidora dos seus direitos fundamentais.

1.1.2 A proteção de dados pessoais como um aprofundamento da proteção à privacidade.

Como a proteção à privacidade é a grande questão de princípio a nortear esta pesquisa e, considerando que é do seu aprofundamento que surge o referido direito à proteção de dados pessoais, é essencial compreender a função dos princípios no âmbito do pós-positivismo.

Nesse sentido, Dworkin (2011, p. 36-39) afirma que a sua

> [...] estratégia será organizada em torno do fato de que, quando os juristas raciocinam ou debatem a respeito de direitos e obrigações jurídicas, eles recorrem a padrões que não funcionam como regras, mas operam diferentemente, como princípio, políticas e outros tipos de padrões[15]. [...] A diferença entre princípios jurídicos e regras jurídicas[16] é de natureza lógica. Os dois conjuntos de padrões apontam para decisões particulares acerca da obrigação jurídica em circunstâncias específicas, mas distinguem-se quanto à natureza da orientação que oferecem. As regras são aplicáveis à maneira do tudo-ou-nada. Dados os fatos que uma regra estipula, então ou a regra é válida, e neste caso a resposta que ela fornece deve ser aceita, ou não é válida, e neste caso em nada contribui para a decisão.

Apesar das divergências doutrinárias entre ambos, esta distinção – entre regras e princípios – também é feita por Robert Alexy (2008, p. 85), para quem a compreensão das

---

[14] Por intervenções cosméticas se entende aquelas pouco efetivas que são feitas apenas como forma de satisfazer a opinião pública, servindo como fundamentos para um discurso de segurança que não pode ser atingido, tendo em conta os riscos socialmente produzidos (BECK, 2010).

[15] Dworkin explica que: 'política' seria "aquele tipo de padrão que estabelece um objetivo a ser alcançado, em geral uma melhoria em algum aspecto econômico, político ou social da comunidade (ainda que certos objetivos sejam negativos pelo fato de estipularem que algum estado atual deve ser protegido contra mudanças adversas)." (2011, p. 36) Por outro lado 'princípio' é "um padrão que deve ser observado, não porque vá promover ou assegurar uma situação econômica, política ou social considerada desejável, mas porque é uma exigência de justiça ou equidade ou alguma outra dimensão da moralidade." (2011, p. 36)

[16] Deste modo "Os princípios possuem uma dimensão que as regras não têm – a dimensão do peso ou importância. Quando os princípios se intercruzam, aquele que vai resolver o conflito tem de levar em conta a força relativa de cada um. Esta não pode ser, por certo, uma mensuração exata e o julgamento que determina que um princípio ou uma política particular é mais importante que outra frequentemente será objeto de controvérsia." (DWORKIN, 2011, p. 42) Por outro lado "As regras não têm essa dimensão. Podemos dizer que as regras são funcionalmente importantes ou desimportantes [...] Se duas regras entram em conflito, uma delas não pode ser válida. A decisão de saber qual delas é válida e qual deve ser abandonada ou reformulada, deve ser tomada recorrendo-se a consideração que estão além das próprias regras. Um sistema jurídico pode regular esses conflitos através de outras regras, que não precedência à regra formulada por uma autoridade de grau superior, à regra promulgada mais recentemente, à regra mais específica, ou outra coisa do gênero." (DWORKIN, 2011, p. 43)

normas que tratam de direitos fundamentais – como é o caso da proteção à privacidade – deve partir da distinção, dentro do gênero normas, de duas espécies: as regras[17] e os princípios[18].

Consideradas estas distinções feitas pelos autores, pode-se afirmar que a "proteção à privacidade" é uma norma que essencialmente trata de um direito fundamental, decorrente da dignidade da pessoa humana. Possui caráter de garantia do exercício dos demais direitos civis e políticos, pois possibilita a construção livre da personalidade individual. Assim ela tem um conteúdo amplo e, portanto, tem a natureza de princípio, tanto para Dworkin quanto para Alexy.

Já a idéia de "proteção aos dados pessoais" surge como uma norma decorrente do aprofundamento do direito fundamental à defesa e promoção da "privacidade", sem perder a "proteção aos dados" a natureza de princípio. Desse modo, este princípio não pode ser compreendido como algo complemente autônomo, pois a força dentro da moralidade política e da historicidade jurídica que a privacidade tem decorreu de séculos de construção jurídica que não podem e nem devem ser desconsiderados.

Da mesma forma, é necessário classificar os princípios constitucionais (BARROSO, 2009, p. 318) como: princípios fundamentais – quando expressam decisões políticas essenciais do constituinte, princípios gerais – que seriam pressupostos ou especificações dos princípios fundamentais e, por fim, os princípios setoriais – que incidirão sobre determinadas situações específicas.

No caso concreto, a proteção à privacidade apresenta um caráter de princípio geral, que decorre do princípio fundamental da dignidade da pessoa humana, expresso no artigo 1º parágrafo único da Constituição Federal. Nessa linha de raciocínio e seguindo os ensinamentos de Barroso (2009), a proteção de dados pessoais pode ser entendia como um princípio setorial decorrente do princípio geral da proteção da privacidade.

Ainda, a proteção à privacidade caracteriza-se como tendo uma "fundamentalidade material", isto é, tem um conteúdo que a torna uma norma de *status* superior. Conteúdo este decorrente de sua essencialidade para a formação da personalidade individual e naturalmente para o gozo dos demais direitos civis e políticos.

---

[17] Para Alexy (2008, p. 91) "as regras são sempre ou satisfeitas ou não satisfeitas. Se uma regra vale, então, deve se fazer exatamente aquilo que ela exige; nem mais, nem menos. Regras contêm, portanto, determinações no âmbito daquilo que é fática e juridicamente possível.".

[18] Da mesma forma "os princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes, e, por conseguinte eles são mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídica." (ALEXY, 2008, p. 91)

Como esclarece Ingo Sarlet (2009, p. 75-77), quanto a esta referida fundamentalidade dos direitos fundamentais,

> [...] somente a análise do seu conteúdo permite a verificação de sua fundamentalidade material, isto é, da circunstância de conterem, ou não, decisões fundamentais sobre a estrutura do estado e da sociedade, de modo especial, porém no que diz com a posição nestes ocupada pela pessoa humana. [...] Direitos fundamentais são, portanto, todas aquelas posições jurídicas concernentes às pessoas, que, do ponto de vista do direito constitucional positivo, foram por seu conteúdo e importância (fundamentalidade material), integradas ao texto da constituição e, portanto, retiradas da esfera de disponibilidade dos poderes constituídos (fundamentalidade formal).

Em decorrência desta fundamentalidade material, surge a exigência de aprofundamento deste princípio de "proteção à privacidade", sobretudo se considerado o risco que o desenvolvimento e a utilização massiva das TIC trouxeram, e, portanto, evidencia-se a necessidade de se repensar os mecanismos de sua proteção.

Para além desta fundamentalidade, é importante referir ainda que os princípios têm uma eficácia interpretativa[19] que consiste "em que o sentido e alcance das normas jurídicas em geral devem ser fixados tendo em conta os valores e fins abrigados nos princípios constitucionais." (BARROSO, 2009, p. 319).

Desta forma, a ausência de uma previsão normativa específica não deve impedir que a interpretação de determinado princípio seja aprofundada, sobretudo quando em confronto com uma nova realidade que tende a fragilizar tal norma.

Para os autores civilistas tradicionais, a proteção aos direitos de personalidade historicamente esteve atrelada a uma visão de direito privado desvinculada do papel constitucional que estes direitos possuem, como se a sua força normativa decorresse exclusivamente de previsões positivas nos códigos.

Porém, com o fenômeno da constitucionalização do Direito[20], esta forma de interpretar estes direitos merece dar lugar à visão de que a proteção deles traz consigo um caráter de defesa de direitos fundamentais e, portanto, o intérprete não pode e nem deve, dentro de um Estado Democrático de Direito, limitar-se pelas previsões das regras infraconstitucionais.

---

[19] Como esclarece Luiz Roberto Barroso (2009, p. 363) "Ao aplicar a norma o intérprete deverá orientar seu sentido e alcance à realização dos fins constitucionais. Em suma: a Constituição figura hoje no centro do sistema jurídico, de onde irradia sua força normativa, dotada de supremacia formal e material. Funciona assim não apenas como parâmetro de validade, mas também como vetor de interpretação de todas as normas do sistema.".

[20] Deste modo, "A idéia da constitucionalização do Direito aqui explorada está associada a um efeito expansivo das normas constitucionais, cujo conteúdo material axiológico se irradia, com força normativa, por todo o sistema jurídico. Os valores, fins públicos e os comportamentos contemplados nos princípios e regras da Constituição passam a condicionar a validade e o sentido de todas as normas de direito infraconstitucional." (BARROSO, 2009, p. 352)

Desse modo, é possível estabelecer a revolução informacional e a sociedade que ela deu origem como cenário onde a noção de proteção de dados pessoais, como um direito fundamental, se desenvolve a partir do aprofundamento do princípio da proteção à privacidade.

Dentro deste cenário, a ideia de proteção à privacidade prevista nas convenções internacionais, diretivas comunitárias e legislações nacionais, exige que esta privacidade seja preservada por meio de um direito autônomo, denominado proteção de dados[21].

O necessário aprofundamento da privacidade decorre da sua cada vez mais frágil forma de proteção – inicialmente considerada como um mero '*direito de ser deixado só*' – que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito (RODOTÁ, 2008, p. 24), o que significa a compreensão da privacidade, a partir do seu aprofundamento como proteção de dados pessoais.

Como ensina Rodotá (2008, p. 32):

> De discurso fechado nas fronteiras de uma classe, a privacidade se projeta sobre a coletividade, E o cadastramento de grandes contingentes populacionais – fenômeno que parece pressupor sua morte – está na origem de uma transformação qualitativa que pode permitir que a privacidade recupere sua carga vital e assuma funções antes desconhecidas.

A partir desta realidade, podem ser imediatamente extraídas duas consequências: a primeira relativa à possibilidade de um 'uso democrático' dos computadores, que parece evidentemente condicionada não só à qualidade do sujeito gestor, mas também à amplitude do controle coletivo exercido sobre tais gestões e, em um segundo momento, outra referente à necessidade imediata de realizar uma reforma radical das instituições que controlam as informações (RODOTÁ, 2008, p. 33).

A primeira, para o presente tema, refere-se ao avanço das regras relativas ao acesso às informações públicas, o que pode gerar uma maior fiscalização sobre os sujeitos gestores dos bancos de dados pessoais, fazendo com que a privacidade dos titulares de tais informações seja protegida de forma mais efetiva.

Já a segunda, dentro desta temática, refere-se à necessidade de uma reestruturação das próprias instituições que tratam da utilização e do tratamento destes dados para que esta

[21] O direito à proteção de dados como um direito autônomo em relação à privacidade inicialmente esteve previsto no artigo 35 da Constituição Portuguesa de 1974 e no artigo 18.4 da Constituição Espanhola de 1978, posteriormente na Convenção nº 108 do Conselho da Europa, e nas Diretivas 1995/46, 1997/66, 2002/58 e 2006/24 do Parlamento Europeu e do Conselho da Europa.

atividade se torne mais democrática e legítima, o que resultará na proteção da privacidade das pessoas que integram toda a coletividade.

Esta forma de compreensão – de proteção de dados como aprofundamento do princípio da privacidade –, está motivada, em um primeiro momento, pelo número e pelo grau das lesões e violações ocasionadas pelo uso de TIC, o que exige o seu tratamento como um direito autônomo e, em um segundo momento, pela forma de atuação que se espera para a proteção deste direito específico.

Enquanto o direito à privacidade – como "*direito de ser deixado só*" – sempre exigiu mera proteção negativa, a proteção de dados necessita de uma ação positiva, isto é, de defesa deste direito por meio de regulamentação das formas de intervenção e pela garantia de autodeterminação informativa[22], e não simplesmente impossibilitando que esta ocorra.

Nesta nova realidade, utilizar estratégias não equilibradas para solucionar a questão da privacidade, dadas as suas peculiares características já tratadas, não contribui para uma maior proteção do sujeito, como esclarece Stéfano Rodotá (2008, p. 25):

> Não é mais possível considerar os problemas da privacidade somente por meio do pêndulo entre 'recolhimento' e 'divulgação', entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a 'casa-fortaleza', que glorifica a privacidade e favorece o egocentrismo, e a 'casa-vitrine', que privilegia as trocas sociais; assim por diante.

A evolução do conceito de privacidade, a partir da década de 1960, passou a relacionar-se diretamente com a proteção de informações pessoais, exigindo-se uma prestação positiva para sua proteção.

Na Europa, a proteção de dados pessoais recebeu status constitucional com o artigo 35 da Constituição Portuguesa de 1974 (PORTUGAL, 2014), onde foi estabelecido que: "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei"

Da mesma forma o artigo 18.4 da Constituição Espanhola de 1978 (ESPANHA, 2014), previu que: "A lei limita o uso da tecnologia da informação para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos"

[22] Conceito essencial para o presente tema, que é tratado por autores como Pérez Luño (2011), Têmis Limberger (2007) e Stéfano Rodotá (2008), e que significa uma garantia de que o titular de determinado dado deverá ter um conhecimento razoável sobre as utilizações que serão feitas com tal informação, como tratado com mais profundidade mais a frente quando do tratamento da "vulnerabilidade de dados pessoais em face da segmentação" no ponto 1.3.

Ainda, no nível da Comunidade Europeia, é na década de 80, com a Convenção nº 108 do Conselho da Europa (UNIÃO EUROPEIA, 2014), que se inicia o reconhecimento e um direito fundamental à proteção da privacidade a partir da proteção de dados pessoais. No artigo 1º do referido documento há a previsão de que:

> A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito (proteção dos dados).

Em 1995, com a adoção da Diretiva 1995/46 do Parlamento Europeu e do Conselho da Europa (UNIÃO EUROPEIA, 2014-A), os países europeus passam a organizar um sistema mínimo de segurança e de proteção de dados pessoais a nível comunitário, conforme previa o Artigo 1º: "1. Os estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais."

Após este documento, houve a Diretiva 1997/66 (UNIÃO EUROPEIA, 2014-B), que buscando harmonizar o tratamento da questão dos dados pessoais pelos estados membros em seu artigo 1º previu:

> [...] a harmonização das disposições dos estados-membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das telecomunicações e para garantir a livre circulação desses dados e de equipamentos e serviços de telecomunicações na Comunidade.

Posteriormente foi editada a Diretiva 2002/58, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas (UNIÃO EUROPEIA, 2014-C), que estabeleceu em seu artigo 1º:

> A presente directiva harmoniza as disposições dos estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das comunicações electrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações electrónicas na Comunidade

Por fim, sobreveio a Diretiva 2006/24 (UNIÃO EUROPEIA, 2014-D), relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, que altera a Diretiva 2002/58/CE, prevendo no Artigo 1º que:

> 1. A presente directiva visa harmonizar as disposições dos estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito nacional de cada estado-Membro.

Observa-se nestas Diretivas a necessidade de harmonização das legislações dos Estados Partes, necessidade que vai ao encontro da proteção de dados pessoais dentro do ambiente virtual, na medida em que, perante a rede mundial de computadores, de pouco valem as fronteiras nacionais.

Desse modo, qualquer tentativa, em âmbito nacional, de estabelecer um marco regulatório capaz de proteger os dados pessoais individuais dos internautas deve estar adequada às legislações dos demais países, sob pena de ser juridicamente ineficaz, considerando que os dados podem instantaneamente transitar dentro do espaço virtual que não está localizado necessariamente dentro do território de qualquer dos estados nacionais.

Além disto, os maiores intermediários do acesso à *Internet* geralmente estão concentrados em determinados estados nacionais e, como intermediários – dentre os quais os provedores de acesso, essenciais para o presente trabalho – acabam captando e manejando uma imensa quantidade de dados pessoais de indivíduos que não necessariamente estão dentro destas mesmas fronteiras nacionais. Então, a proteção de dados necessita essencialmente de uma harmonização de tratamento normativo.

Tal harmonização de tratamento consiste em uma das principais justificativas do presente estudo comparado, que objetiva analisar a condição de proteção do internauta latino-americano, nos países analisados, integrantes do Mercosul.

Além disto, dentro de um mesmo bloco econômico – como é o caso do Mercosul – a harmonização na regulamentação da proteção de dados pessoais ganha um elevado grau de importância se considerar que estes países tendem à integração econômica e política e, portanto a um trâmite cada vez mais intenso de dados pessoais dos seus cidadãos.

Quanto ao conceito de dados, Catarina Sarmento e Castro (2005, p. 74) entende que os dados pessoais, podem ser assim denominados

> [...] quando permitem identificar uma pessoa – desde logo se surgem associados a um nome –, as suas classificações escolares, curriculum, a sua história clínica, as suas dívidas e créditos, as compras que efetua, o registro dos meios de pagamento que utiliza.

Maria Eduarda Gonçalves (2003, p. 89) define dados pessoais, em conformidade com a Convenção do Conselho da Europa, como sendo "qualquer informação relativa a uma pessoa física identificada ou identificável (artigo 2º). Uma pessoa física não é considerada identificável se a sua identificação requer tempo, custos ou atividades exageradas."

Ainda, estes dados podem ser classificados como sendo sensíveis ou de caráter pessoal[23] ou não sensíveis, e a depender desta classificação, o nível de proteção será diverso.

Enfim, absolutamente tudo (KAKU, 2000, p. 90) que trafega na *Internet* é dado. Não importa que seja uma simples pesquisa ou cadastro que se aceita fazer através da rede, ou ainda imagens que possam ser armazenadas sob qualquer meio ou forma. Na realidade tudo consiste em informação armazenada, independente do tempo e que diga respeito aos atos e fatos do dia-a-dia dos indivíduos.

Essa ampla gama de informações disponíveis e disponibilizáveis traz dados detalhados sobre a particularidade de cada pessoa, suas preferências e gostos, enfim, informações pertencentes à proteção de dados. Observa-se que a regulação da privacidade é primordial também para acabar condicionando as ações presentes e futuras de empresas e de governos frente ao uso da tecnologia da informática.

Deste modo, é essencial um profundo processo de revisão dos critérios de classificação das informações pessoais, segundo uma escala de valores renovada (RODOTÁ, 2008, p. 35). Dentro desta escala, deve ser garantido o máximo de opacidade às informações suscetíveis de originar práticas discriminatórias e, por outro lado, o máximo de transparência àquelas que, referindo-se à esfera econômica[24] dos sujeitos, concorrem para embasar decisões de relação coletiva.

Em todo o caso, sempre deve ser resguardada a inviolabilidade daquele dado pessoal cuja divulgação possa ocasionar violação a direitos constitucionais do titular, como afirma (KAKU, 2000, p. 91):

> A inviolabilidade do sigilo de dados é ponto capital, também, para que certas regras sejam seguidas dentro do meio digitalizado, tudo que trafega na

[23] Esta classificação de dados entre sensíveis ou pessoais e não sensíveis é essencial para o presente trabalho, como esclarece Gonçalves (2003, p. 90): "O conteúdo dos próprios dados é também suscetível de determinar um maior ou menor grau de risco para os indivíduos a que os dados dizem respeito. [...] A Convenção estabelece que os dados de caráter pessoal que revelem origem racial, as opiniões políticas, as convicções religiosas ou outras convicções, assim como os dados pessoais relativos à saúde ou a vida sexual, não podem ser tratados automaticamente, a menos, que o direito interno preveja garantias apropriadas. O mesmo regime aplica-se aos dados de caráter pessoal relativos a condenações penais (artigo 2º)".

[24] Tais como as condições de vulnerabilidade econômica e social, capazes de possibilitar a identificação da necessidade de uma efetiva intervenção para garantia de um mínimo de direitos sociais, econômicos e culturais, seja através de políticas públicas ou mesmo por meio de programas de assistências que partam da iniciativa privada.

> *Internet* é dado [...] O direito constitucional garantidor de tais direitos individuais está à disposição da sociedade, a fim de coibir que as práticas públicas e privadas na esfera do manuseio da tecnologia da informática sejam abusivas, através de circunstâncias e parâmetros mais humanamente civilizados em detrimento do economicamente liberalizado.

Para Têmis Limberger (2007, p. 58), a informação atualmente é uma riqueza fundamental da sociedade, e os programas interativos criam uma nova mercadoria. Dessa forma, o sujeito fornece os dados de maneira súbita e espontânea e, por conseguinte, depois que estas são armazenadas, esquece-se de que os relatou.

Assim, a caracterização da sociedade como cada vez mais baseada sobre acumulação e a circulação das informações comporta o nascimento de um novo e verdadeiro 'recurso' de base, ao qual se coliga ao estabelecimento de novas situações de poder (RODOTÁ, 2008, p. 35). Por exemplo, sustenta-se que a coleta de dados utilizada pelos poderes públicos para tomar decisões que dizem respeito a programas de desenvolvimento[25], contendo exclusivamente dados agregados, não é perigosa para a privacidade, já que, para esses dados, não seriam necessários controles especiais ou o reconhecimento aos indivíduos de um direito de acesso (RODOTÁ, 2008, p. 32).

Porém, mesmo as coletâneas de dados anônimos podem ser manipuladas de forma gravemente lesiva aos direitos dos indivíduos: tenha-se em mente o uso que pode ser feito dos dados agregados que digam respeito a uma minoria racial ou linguística, ou às consequências de uma decisão política ou econômica tomada justamente com base na análise dos dados anônimos.

Dessa forma, dentro da sociedade informacional, a proteção de dados pessoais é considerada um direito fundamental e deve ser ponderada em face de outros valores igualmente importantes para sociedade, como a segurança individual e coletiva, sob pena de uma vulneração de direitos civis que não pode ser constitucionalmente aceita.

1.1.3 A ampliação do controle e da vulnerabilidade de direitos na sociedade informacional.

A proteção de dados pessoais, que está fundada nas noções de dignidade da pessoa humana e de liberdade individual, tem sido contraposta à ideia de vigilância e controle, que é justificada partir da noção de segurança coletiva e individual.

---

[25] Tal situação, considerando a realidade brasileira que convive com diversos programas governamentais assitencialistas, torna-se preocupante, visto que o governo acaba por captar a condição social e econômica de um número indeterminado de indivíduos.

Com Castells (2003-C, p. 141), verifica-se que "TIC de liberdade estão sendo opostas à tecnologias de controle, a sociedade civil chega às trincheiras de novas batalhas pela liberdade".

Esta noção de segurança coletiva, em uma realidade que vivencia o aumento gradativo da criminalidade e do terrorismo transnacional, acaba recebendo uma importância excessiva, o que passa a justificar a atuação de vigilância e controle por parte do Estado – e por que não dizer de empresas privadas que prestam serviços na área de segurança a este Estado.

Como afirma Pérez Luño (2011 p. 107),

> [...] para combater as novas formas de criminalidade aprimorados através da *Internet*, têm sido criados poderosos sistemas de segurança do estado[26]. Estes sistemas projetaram mecanismos de pesquisa e inteligência para enfrentar os novos desafios.

No entanto, o próprio autor lembra que estes sistemas constituem-se em uma ameaça preocupante para as liberdades civis, tornando-se mecanismos de controle social e de violação da privacidade. Além disso, a operação desses sistemas nem sempre cumpre as exigências das sociedades democráticas, uma vez que, na prática, para levar segurança aos cidadãos exige-se deles a aceitação da intrusão em seus direitos (PÉREZ LUÑO, 2011 p. 107).

Com Bauman (2008, 10-11) é possível afirmar que:

> O estado, por exemplo, tendo encontrado sua raison d'être e seu direito à obediência dos cidadãos na promessa de protegê-los das ameaças à existência, porém não mais capaz de cumpri-la nem de reafirmá-la responsavelmente em vista da rápida globalização e dos mercados crescentemente extraterritoriais -, é obrigado a mudar a ênfase da "proteção contra o medo" dos perigos à segurança social para os perigos à segurança pessoal. O estado então "rebaixa" a luta contra os medos para o domínio da "política de vida", dirigida e administrada individualmente, ao mesmo tempo em que adquire o suprimento de armas de combate no mercado de consumo.

O medo de atos de violência e terrorismo, em conjunto com a possibilidade de controle e vigilância que as TIC trazem, acaba justificando intervenções à liberdade individual, aceitas como parte da atuação dos entes responsáveis pela segurança da sociedade.

Tal fenômeno de massificaçaõ dos medos é exemplificado por Bauman (2008, p. 11):

---

[26] Pérez Luño apresenta dois exemplos destes sistemas: O sistema *Echelon* que "[...] é um sistema de intercepção de comunicações mundiais desenvolvido em conjunto pelos estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia. Sua principal característica, em comparação com outros sistemas de vigilância, é a sua capacidade de exercer controle simultâneo de todas as comunicações." E o sistema *Carnivore* que "[...] é um sistema de hardware e software com a capacidade de localizar e processar comunicação de um usuário da *Internet*. O sistema de comunicação é envolvido em ponto estratégico, como um provedor de serviços de *Internet*." (2011 p. 107).

> Na realidade, o que mais amedronta a sociedade é a ubiquidade dos medos; eles podem vazar de qualquer canto ou fresta de lares e do planeta. Das ruas escuras ou das telas luminosas dos televisores. Dos quartos e das cozinhas. Dos locais de trabalho e do metrô tomado para ir e voltar. De pessoas que são encontradas e de pessoas que não o são. De algo que é ingerido e de algo com o qual os corpos entraram em contato. Da "natureza" (pronta, como dificilmente antes na memória coletiva, a devastar lares e empregos e ameaçar destruir os corpos com a proliferação de terremotos, inundações, furacões, deslizamentos, secas e ondas de calor) ou de outras pessoas (prontas, como dificilmente antes na memória coletiva, a devastar lares e empregos e ameaçando destruir os corpos com a súbita abundância de atrocidades terroristas, crimes violentos, agressões sexuais, comida envenenada, água ou ar poluído)

As oportunidades de ter medo estão entre as poucas coisas que não se encontram em falta na atualidade, altamente carente em matéria de certeza, segurança e proteção. Os medos são muitos e variados. Pessoas de diferentes categorias sociais, etárias e de gênero são atormentadas por seus próprios medos (BAUMAN, 2008, p. 31).

Em face desta gama quase infindável de medos, a população permite a supressão dos seus direitos fundametnais, em prol de evitar os riscos que esta mesma sociedade cria para si.

As informações pessoais tornam-se cada vez mais a grande arma à disposição dos entes de controle para conhecer a todos em todas as suas nuances, tanto pelo discurso adotado quanto pelas suas interações. A necessidade de controlar os riscos e ataques acaba se tornando a justificativa para legitimar as ações dos estados e também das empresas, no pretenso sentido de evitar os imensos e impensáveis riscos a que a sociedade atual esta submetida.

Na atualidade tem-se adquirido consciência de que a informação é poder e que esse poder é decisivo quando, em razão do avanço da informática, converte informações parciais e dispersas em informações em massa e organizadas. E nestas situações não seria aceitável, para este discurso, negar aos poderes públicos o emprego das TIC, quando a intenção desses poderes é a proteção da coletividade dos mais diversos medos socialmente produzidos.

O enorme aumento da quantidade de informações pessoais (RODOTÁ, 2008, p. 28) coletadas por instituições públicas e privadas visa, sobretudo, a dois objetivos: a aquisição dos elementos necessários à preparação e gestão de programas de intervenção social por parte dos poderes públicos, e o desenvolvimento de estratégias empresariais privadas.

Nas sociedades avançadas e complexas do presente (PEREZ LUÑO, 2005, p. 361), a eficácia da gestão administrativa, a erradicação de atividades antissociais e delitivas cada vez mais sofisticadas e a própria moralização da vida cívica exigem contar com um amplo e organizado sistema informativo.

Nas palavras de José Afonso da Silva (2007, p. 209), “O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de

formar grandes bancos de dados, que desvendem a vida dos indivíduos sem sua autorização e até sem seu conhecimento".

A vigilância mais eficaz é aquela que ocorre independente da consciência do cidadão, o que tornou-se mais acessível com o uso das tecnologias informáticas, pela sua complexidade de funcionamento e facilidade de obtenção, tratamento e transmissão de informações.

Para uma compreensão precisa de onde surge esta perspectiva de estado vigilante de tudo e de todos, como forma de manutenção da segurança pública, é necessário referenciar as concepções políticas que surgiram no último século e que, de certa forma, moldaram esta forma de agir.

Em um primeiro momento, é possível observar, nos estados liberais e capitalistas, a concepção política de um "Estado-Gerente" (CHATELET; KOUCHER, 1983, p. 80), que tem a intenção de justificar a sua atuação ou ausência de ação através de um discurso de proteção de determinados valores que dificilmente são questionados, tais como o humanismo, o pluralismo, o reformismo e, por que não afirmar, da segurança coletiva e individual, através do vigilantismo, que, com base nessas justificativas, legitimam seu controle sobre os fluxos de dados e informações produzidas pelos indivíduos.

Outra concepção política que o século XX desvelou foi a concepção de "Estado-Partido" (CHATELET E KOUCHER, 1983, p. 198-9), que surge como reação à concepção anterior e os problemas sociais que ela ocasionou, sobretudo pela má distribuição das riquezas e pelo predomínio nos espaços políticos pelas classes economicamente dominantes. Esta forma de estado, por questões políticas, adotou uma perspectiva de vigilância como forma de evitar eventuais oposições políticas à ideologia que a fundamentava, o socialismo. Assim os estados que adotavam esta concepção vigiavam indivíduos e organizações que poderiam se contrapor ao regime socialista, impedindo qualquer oposição à ideologia política que estava no poder.

Uma terceira concepção política é a perspectiva de "Estado-Nação". Defende a atuação estatal voltada para a comunidade internacional, em uma ótica imperialista (CHATELET; KOUCHER 1983, p. 293). E nesta concepção, o vigilantismo estatal ganha contornos de política institucional estabelecida que, para além de garantia da segurança coletiva e individual e de manutenção do discurso político-ideológico adotado pelo Estado, torna-se uma forma de garantir a continuidade das intervenções internacionais praticadas pelos estados dominantes.

Tal vigilantismo, aliado à visão colonialista, tornou-se mundialmente reconhecido após as revelações da espionagem interestatal realizada pelas agências de inteligência norte-americanas que, segundo relatos de um ex-agente do serviço secreto daquele país, espionavam governos, pessoas e empresas localizadas em outros países em desenvolvimento[27].

Por fim, a última concepção identificada constitui-se em um "Estado-Cientista" (CHATELET; KOUCHER, 1983, p. 447). Surge de uma evolução das concepções anteriores e, principalmente, da tentativa de solucionar as lacunas existentes nas mesmas através de um discurso racional fundamentado na lógica científica. Desta forma a perspectiva da evolução científica e tecnológica une-se à necessidade de vigilância da sociedade, pois dentro desta concepção política estatal, se existissem tecnologias capazes de obter, armazenar, organizar e compartilhar informações pessoais sobre a população, não haveria lógica racional em não utilizá-las.

Portanto, as principais concepções políticas do século XX, de uma forma ou de outra, praticaram a vigilância massiva da população. A grande questão é que a lógica do "Estado-Cientista" se utiliza do funcionamento das TIC como forma de potencializar essa vigilância.

Toda a revolução política é um drama, mas a revolução técnica que se anuncia é, sem dúvida, mais que um drama; é uma tragédia do conhecimento, a confusão babeliana dos saberes. "Como língua de escopo, a *Internet* é ao mesmo tempo a melhor e a pior coisa do mundo. O progresso de uma comunicação sem limites ou quase sem limites e o desastre, a colisão, mais dia menos dia deste Titanic com um *iceberg*" (VIRILIO, 1999, p. 105).

E, portanto, após a bomba atômica, capaz de desintegrar a matéria pela energia da radioatividade, surge, ao fim do milênio passado, o espectro da segunda bomba, a bomba informática que, para Paul Virilio (1999, p. 65), teórico sabidamente tecnofóbico, é capaz de desintegrar a paz das nações pela interatividade da informação.

Uma sociedade hipervigiada pelos entes estatais já foi objeto de diversas obras clássicas da literatura internacional.As mais famosas e importantes foram "1984", de George Orwell e "Admirável Mundo Novo", de Aldous Huxley. Nessas duas distopias, a sociedade sofre tanto com a vigilância que acaba por aceitar esta condição como algo natural de sua existência.

---

[27] Conforme notícia publicada no site de notícias G1: "O ex-técnico da CIA Edward Snowden, de 29 anos, é acusado de espionagem por vazar informações sigilosas de segurança dos estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana – utilizando servidores de empresas como Google, Apple e Facebook – e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da presidente Dilma Rousseff com seus principais assessores" (GLOBO, 2014).

Em “1984”, George Orwell (2009) constrói uma sociedade onde todos são vigiados a todo o instante por um ente denominado “Grande Irmão”. Em absolutamente todas as atividades, monitores e câmeras passam a habitar a integralidade dos locais como forma de manter o controle sobre a totalidade do comportamento dos habitantes e, aqueles que não se comportam adequadamente, acabam excluídos.

Por outro lado, em “Admirável Mundo Novo”, Aldous Huxley (2009) estrutura uma sociedade onde a predisposição genética e os condicionamentos psicológicos determinam qual o comportamento esperado de cada indivíduo, que passa a ser organizada em castas sociais que não se comunicam. Para mantê-la sob controle, a sociedade é constantemente vigiada.

Virilio (1999, p. 118) alerta que essa visão literária não estaria tão distante da realidade como se poderia crer:

> Assim, depois do desenvolvimento das redes de transportes no século XIX e, mais tarde, no século XX, logo teremos, com a rede das redes, a *Internet*, as verdadeiras redes de transmissão da visão do mundo, infovias do áudio visual dessas câmeras *on line* que contribuirão, no século XXI, para desenvolver a televigilância PANÓPTICA (e permanente) dos lugares e das atividades planetárias, que certamente conduzirá para a utilização das redes de realidade virtual.

Porém o grande risco atualmente não é a vigilância estatal, pois pode ter o seu controle submetido aos princípios decorrentes da transparência administrativa dentro de estados democráticos, mas sim a vigilância feita por empresas privadas.

Como afirma Castells (2003-B, p. 350),“a verdadeira questão é outra, se trata do levantamento de informações sobre as pessoas pelas empresas comerciais e organizações de todos os tipos e na criação de um mercado para essas informações”.

Na rede mundial de computadores, coexistem empresas especializadas em coletar e distribuir informações pessoais, tais como nomes, endereços e dados demográficos para uma futura utilização econômica destas informações.

Atualmente visualiza-se uma nova realidade, onde cada compra feita, cada lugar visitado, cada palavra dita e tudo que é lido ou escrito está rotineiramente sendo gravado e armazenado para posterior análise (KAMINSK, 2000, p. 97).

Existe uma tecnologia desenvolvida especificamente para captura destes dados, e a grande maioria das entidades não tem conhecimento técnico suficiente para saber como gerenciá-los de forma leal e justa. Assim, parte da vida das pessoas pode ser monitorada, e outra parte investigada.

Identificando esta realidade e fazendo uma referência à obra de Orwell, Castells (2003-B, p. 350) afirma que atualmente em vez do “Grande Irmão” opressor, tem-se uma

série de “Irmãzinhas” que procuram ser simpáticas, estabelecendo uma relação pessoal com os indivíduos por saberem quem eles são, invadindo suas vidas das mais variadas formas e aspectos.

Dessa forma ele consegue visualizar o grande paradoxo da relação, estas “irmãzinhas” – empresas que proveem acesso a conteúdos – através do monitoramento dos gostos e preferências, traçam o perfil dos seus usuários e utilizam-se deste conhecimento para estabelecer uma relação de confiança onde este próprio usuário se sente à vontade em manter esta relação e, inclusive, fornece uma quantidade cada vez mais expressiva dos seus dados, conforme será evidenciado na sequência.

1.2 DO MARKETING RELACIONAL À SEGMENTAÇÃO COMPORTAMENTAL: UM ESTUDO DAS PRÁTICAS EMPRESARIAIS QUE UTILIZAM NOÇÕES DE PSICOLOGIA COMPORTAMENTAL.

Levando-se em conta os cenários sociais formados pela Revolução Informacional, bem como as transformações jurídicas do conceito de privacidade tratadas anteriormente, é essencial passar à análise do objeto deste capítulo, isto é, a segmentação comportamental.

Tal tema é tratado de forma tímida pela a ciência jurídica, ao contrário das demais áreas das ciências humanas e sociais, como a Comunicação Social e a Psicologia, tendo em vista a sua ocorrência cada vez mais corriqueira em uma sociedade profundamente alterada pela utilização massiva das TIC e a sua possibilidade de motivar uma violação cada vez mais intensa dos dados pessoais.

Deste modo, para possibilitar a compreensão deste fenômeno, será necessário o estudo da temática utilizando premissas teóricas e categorias conceituais de outras áreas, dentre elas a Publicidade e Propaganda, em específico o *Marketing* relacional, e a Psicologia, dentro da tendência Cognitivo-Comportamental.

A divisão do presente subcapítulo justifica-se pela necessidade de que tal fenômeno seja estudado considerando os sujeitos que o praticam, ou seja, as empresas que segmentam comportamentos e os indivíduos, usuários da *Internet*, que têm seu comportamento segmentado.

Por um lado, é essencial compreender a motivação das empresas ao praticar a segmentação de comportamento dos seus clientes e quais as vantagens que elas obtêm com tal prática. Ainda, teoricamente é essencial estudar quais categorias conceituais fundamentam tal

prática sob o ponto de vista da Publicidade e Propaganda, mais precisamente, do *Marketing* de relacionamento praticado com base em bancos de dados (*Database Maketing*).

Por outro lado, é necessário entender quais os efeitos psicológicos para os sujeitos que acabam submetidos a tal prática e, para tanto, é importante apreender como a Psicologia Comportamental se desenvolveu. Da mesma forma, é preciso compreender, a partir de determinadas categorias conceituais - respondante, operantes, aprendizagem por observação -, como esta corrente da Psicologia explica as reações, muitas vezes inconscientes daqueles que tem o seu comportamento segmentado.

Por fim, compreendida a segmentação comportamental sob o ponto de vista do *Marketing* e da Psicologia, será tratada a base técnica que permite esta prática, ou seja, a questão dos chamados "dossiês digitais", que consistem em grandes bancos de dados pessoais de um número indeterminado de pessoas, obtidos de formas muitas vezes pouco claras, permitindo a ocorrência deste modelo de segmentação.

1.2.1 Novas estratégias empresariais: do marketing de massa ao marketing segmentado.

As empresas são motivadas por interesses econômicos e os produtos ofertados são direcionados à venda. Portanto, logicamente, quanto mais um determinado produto é capaz de ser vendido a uma gama ilimitada de indivíduos, maior quantidade deste produto estará à disposição dos consumidores.

Tal realidade sempre foi inquestionável – sobretudo na era industrial –, pois as empresas produzem os seus produtos e serviços para um grande público e o seu interesse é que estes produtos estejam disponíveis para um número indeterminado e crescente de pessoas.

A Revolução Industrial possibilitou uma produção em série de produtos com as mesmas funcionalidades para atender a um consumidor "médio", isto é, o consumidor em geral, independentemente de suas convicções pessoais, políticas, religiosas,afetivas ou nicho social. O *marketing* – entendido como estratégia para a venda destes produtos – também foi pensado inicialmente como técnica de persuasão do grande público. Para esta forma tradicional de *marketing*, não importava o sujeito que se busca persuadir, mas o grande objetivo era convencer todo e qualquer indivíduo que aquele produto era capaz de satisfazer todas as suas mais variadas e genuínas necessidades e desejos, como decorrência da pesquisa de Pizzinato e Zem (2005, p. 18).

Obviamente, como esclarecem os mesmos autores (2005, p. 19), este *marketing* admitia segmentações de mercado; ora poderia direcionar-se às crianças, ora à mulher, ora aos homens de certa idade, mas sempre tinha uma conotação geral, isto é, ou direcionava-se para

as crianças, ou para as mulheres em geral, dentre outros. Assim, esta forma de *marketing* "de massa" não necessariamente objetivava crianças do sexo masculino de famílias de origem orientais altamente religiosas, ou para mulheres com elevado grau de vaidade com empregos no setor de vendas, propensas à política de esquerda. Os nichos que se apresentavam não eram muito específicos. Isto, dentre outras razões, era decorrência de que os produtos à disposição não eram muito variados. Portanto, o *marketing* que se desenvolvia por tentar abarcar uma gama extremamente complexa e variada de indivíduos acabava sendo pouco persuasivo.

Com a ampliação do acesso que a revolução das TIC permitiu, esta realidade inquestionável – de que quanto maior a quantidade de produtos idênticos à disposição dos consumidores em geral, maior seria o lucro obtido com a venda – começou a transformar-se e este efeito, na visão de autores como Chris Anderson (2006), passou a ser chamada de efeito da "Cauda Longa".

Chris Anderson (2006) cunhou esta expressão ao estudar o mercado do entretenimento junto aos sistemas do *Itunes*, do *Amazon*, do *Netflix*, entre outros, onde constatou que os maiores lucros destas empresas não necessariamente provinham de poucos produtos com um número alto de vendas, mas sim de diversos produtos com um número pequeno, porém constante de vendas.

Segundo Chris Anderson (2006, p. 05),

> Cada vez mais o mercado de massa se converte em massa de nichos [...] Essa massa de nichos sempre existiu, mas com a queda dos custos de acessá-la – para que consumidores encontrem produtos de nicho e produtos de nicho encontrem consumidores –, ela, de repente, se transformou em força cultural e econômica a ser considerada.

O autor afirma que o termo "Cauda Longa" decorre da estatística, onde se determina através de uma curva de demanda que, no decorrer do tempo, os produtos com maior vendagem não necessariamente são os produtos mais lucrativos. Por exemplo, no caso do "*Amazon"*, os livros menos vendidos respondiam por 98% das vendas no período analisado, enquanto os grandes *best sellers* correspondiam a apenas 2% (ANDERSON, 2006, p. 08) .

O referido autor (2006, p. 08) ainda esclarece que "esses nichos são um vasto território ainda não mapeado, com enorme variedade de produtos, cuja oferta até então era antieconômica. Muitos desses produtos estavam lá há muito tempo, mas não eram visíveis ou prontamente identificáveis."

Enfim, essa teoria pode ser resumida como uma nova dinâmica do *marketing* de vendas, da seguinte forma:

> Nossa cultura e nossa economia estão cada vez mais se afastando do foco em alguns hits relativamente pouco numerosos (produtos e mercados da tendência dominante), no topo da curva da demanda, e avançando em direção a uma grande quantidade de nichos na parte inferior ou na cauda da curva de demanda. Numa era sem as limitações do espaço físico nas prateleiras e de outros pontos de estrangulamento da distribuição, bens e serviços com alvos estreitos podem ser tão atraentes em termos econômicos quanto os destinados ao grande público (ANDERSON, 2006, p. 50).

Deste modo, constata-se que a clássica produção em massa de produtos idênticos, com a ampliação do acesso propiciada pelas TIC, passou a dividir espaço com a produção segmentada de determinados produtos e serviços direcionados a determinadas classes de mercado. Estes nichos, por sua vez, tornaram-se cada vez mais específicos e variados, pois as tecnologias possibilitaram uma construção de identidades e personalidades igualmente variadas e, por que não dizer, variáveis.

Assim, o caminho tradicional do *marketing* seria tornar-se segmentado, isto é, abandonar a perspectiva de um *marketing* direcionado à grande população para tornar-se um *marketing* de pequenos grupos consumidores. Nesta perspectiva, seguem os ensinamentos de Pizzinato e Zem (2005, p. 18), que oferecem interessante noção sobre a evolução dessas estratégias:

> Analisando algumas das fases da evolução do marketing, pode-se observar que o marketing de segmentos é uma abordagem que fica entre o marketing de massa e o marketing individual. Com ele, as empresas projetam seus produtos e serviços para um ou mais segmentos específicos, ao invés de fazê-lo de maneira massificada, vislumbrando todo o mercado. (...) Para o marketing de segmentos, a motivação de algumas pessoas para comprar é bem diferente de outras, motivo pelo qual a padronização absoluta tende a não funcionar adequadamente. Na assunção deste enfoque, produtos e serviços passam por processos de adaptação para atendimento de necessidade e desejos específicos de dado perfil de clientes, selecionados dentro de um mercado maior.

Mas como produzir um instrumento de persuasão que pudesse atingir os nichos e segmentos cada vez mais específicos e individualizáveis que surgem na sociedade contemporânea? E como oferecer produtos que não necessariamente são destinados a uma grande massa de indivíduos, produtos específicos para determinados nichos e, ao mesmo tempo, oferecer os produtos tradicionais geralmente produzidos para a grande população?

A solução óbvia é conhecer os gostos de cada indivíduo – entender suas preferências culturais, afetivas, políticas, se está incluído em algum nicho de contracultura, etc. – e direcionar a ele uma publicidade (*marketing*) específica, pois assim aquele produto – independentemente de ser um produto geral ou um produto específico – irá atrair o seu interesse.

Tal solução teoricamente é simples, porém a sua efetivação prática é extremamente complexa, pois como conhecer cada indivíduo, cada nicho, o que ele pensa, sente, gosta, não gosta, ouve, lê, e como pensar em estratégias de *marketing* direcionadas a ele?

Aqui as tecnologias informacionais surgem como uma saída extremamente interessante, sobretudo em uma realidade onde a autoexposição e o fornecimento de dados pessoais torna-se algo cada vez mais arraigado culturalmente.

Surge então a segmentação comportamental que para Frederik Zuiderveen Borgesius (2014, p. 2) significa "[...] o monitoramento que se faz do comportamento das pessoas na *Internet* ao longo do tempo, para usar as informações recolhidas com o intuito de dirigir-lhes publicidade conforme as inferências a respeito de seus interesses".

Essa forma de diferenciação dos comportamentos tem uma clara relação com a Psicologia social e com recentes evoluções do *marketing*, como afirmam Regina Gonçalves Vieira Bueno e Ana Akemi Ikeda (2014, p. 3):

> A partir da perspectiva segundo a qual a compreensão do comportamento do consumidor se dá a partir de suas principais variáveis de influência, uma das primeiras definições de envolvimento data do final da década de 40, estando fortemente associada à Psicologia social.

Portanto o *marketing* de relacionamento esteve desde seu princípio vinculado à Psicologia social, mais precisamente a uma forma de Psicologia *behaviorista* e, atualmente, pode-se dizer Cognitivista Comportamental. Assim as teorias comunicacionais que fundamentaram estas novas formas de *marketing* buscaram nos estudos psicológicos compreender os efeitos do sujeito submetido a esta forma de publicidade. Deste modo:

> Não é por acaso que o termo segmentação está fortemente relacionado a conceitos como diferenciação, satisfação de diferentes nichos e vantagem competitiva, já que todos objetivam cada um à sua maneira, o atendimento às necessidades dos consumidores. (BUENO; IKEDA, 2014, p. 7)

A segmentação comportamental "pode beneficiar empresas e consumidores, mas também traz à baila preocupações acerca da privacidade. As empresas podem compilar perfis detalhados dos usuários da *Internet* com base no que eles leem que vídeos assistem, que buscas fazem, etc." (BORGESIUS, 2014, p. 3)

Conforme notícia publicada no site da revista Época-Negócios (PEPPERS; ROGERS, 2014):

> Com a evolução das tecnologias e das técnicas de segmentação comportamental, centradas na veiculação de anúncios capazes de atrair a atenção do consumidor digital, era inevitável que surgissem questões relacionadas à privacidade

> desse consumidor. Dois grupos de defesa do consumidor, o Grupo de Pesquisas do Interesse Público Americano e o Centro de Democracia Digital, levaram a questão à Comissão Federal do Comércio (FTC). Em uma peça acusatória de 50 páginas, ambos os grupos pedem à FTC que investigue a existência de práticas de segmentação comportamental por parte de grandes empresas que veiculam anúncios em seus sites - Microsoft, Yahoo e Google.

Como se percebe, a segmentação de comportamento preocupa diversas entidades protetoras de direitos civis e consumeristas, o que denota a grande possibilidade de que estas práticas acabem por motivar uma publicidade abusiva[28], que tenta motivar o inconsciente do indivíduo a determinada ação, que conscientemente talvez ele não praticasse.

Ao analisar a prática do envio de anúncios personalizados através de *smartphones*, enquanto o usuário estiver dentro de um *Shopping Center*, Renato Hugo Masina (2014, p. 19) oferece uma definição muito clara sobre a Segmentação comportamental, afirmando que ela "[...] se refere a uma gama de tecnologias e técnicas utilizadas por editores de *siteson line* e anunciantes que buscam aumentar a eficácia de suas campanhas por captura de dados gerados pelo site e pelos visitantes da página".

O cuidado que se deve ter é se esta captura de dados é feita com o conhecimento e consentimento informado do indivíduo titular de tais informações, pois quando realizada sem esses requisitos, pode ser considerada uma quebra de segurança do navegador – ou mesmo do provedor de acesso[29] – sendo ilegal, por violação aos direitos fundamentais deste usuário, sobretudo a proteção de dados.

Dessa forma Masina (2014, p. 21) explica o funcionamento destes sistemas:

> Quando se visita um site, as páginas, a quantidade de tempo que cada página é visualizada, os links clicados, as buscas feitas e as interações realizadas ficam armazenadas, possibilitando que sites coletem os dados para que se crie um 'perfil' dos usuários.

Em decorrência deste perfil dos gestores – no caso os editores do site –, os dados podem ser usados para criar segmentos de público, definidos com base em visitantes que têm perfis semelhantes, para ofertas específicas de produtos com características que possam interessar a este nicho de mercado.

---

[28] Como o autor Cass Sisteins trabalha na obra "Públic.com" (2001).

[29] Conforme o Guia do usuário da *Internet*, organizado pela Rede Nacional de Pesquisa, o provedor de acesso "aquele que se conecta a um provedor de backbone através de uma linha de boa qualidade e revende conectividade na sua área de atuação a outros provedores (usualmente menores), instituições e especialmente a usuários individuais, através de linhas dedicadas ou mesmo através de linhas telefônicas discadas." (BRASIL, 2014, p. 7) Enfim como esclarece Leonardi (2005, p. 22) os provedores de acesso são pessoas jurídicas que possibilitam o acesso dos seus clientes consumidores à *Internet*, elas normalmente devem dispor de uma conexão a um backbone se dentro de sua própria infraestrutura, ou através de uma contratação onerosa.

Desta forma a Segmentação comportamental possibilita uma forma de *marketing*, o chamado *Marketing* Relacional ou Comportamental, especificado como um *marketing* por banco de dados (*Database Marketing*).

E como tal *marketing* é direcionado a um pequeno grupo de indivíduos previamente selecionados pelos seus gostos e preferências, pode ser muito mais ostensivo que o tradicional *marketing* de massa que existia até então.

O *database marketing*, como esclarece Denise Von Poser (2005, p. 36),

> [...] é um conjunto de dados organizados e abrangentes sobre todos os clientes da empresa, incluindo os atuais, os potenciais e até mesmo os não clientes. Esses dados devem estar atualizados e precisam ser de fácil acesso, confiáveis e com alto grau de praticidade a fim de serem utilizados pelas empresas em suas atividades de relacionamento, sejam elas de vendas, marketing ou *call center*, ou ainda qualquer ponto de acesso que o cliente utilize para se comunicar com a empresa.

Nesta forma de *marketing*, qualquer informação incluída no banco de dados requer o maior grau de precisão possível, principalmente as de caráter pessoal (POSER, 2005, p. 40), sendo praticável recorrer a subgrupos cujo objetivo é conhecer as características, os gostos e até as peculiaridades de cada cliente.

Com base nesta divisão, as recomendações às empresas é que pratiquem o que é denominado ‘individualização em massa’, isto é, a partir de algumas características individuais dos atuais ou potenciais clientes, agrupá-los em segmentos de mercado, direcionando a eles um *marketing* específico.

Considerando que o presente capítulo visa analisar as práticas empresarias e tendo em vista de que o principal interesse das empreses é o lucro, obviamente a resposta ao questionamento “Por que utilizar o *Database Marketing*?” é simples. Utiliza-se essa estratégia porque é economicamente mais atraente, uma vez que, de certa forma, garante que as ofertas chegarão àqueles indivíduos que terão uma propensão maior à aquisição dos produtos ou serviços.

Além disso, com o acesso possibilitado pelas TIC, reduzem-se os custos de propaganda, o que exige desta forma de *marketing* um custo inferior ao *Marketing* tradicional, cujo objetivo seria atingir um grande público de acesso irrestrito. Portanto, o *Database Marketing* – ou *Marketing* Segmentado com base em bancos de dados digitais – possibilita às empresas um relacionamento individualizado com os clientes, mesmo que estes não tenham conhecimento disso, o que minimiza os investimentos em *marketing* de vendas, permitindo a venda segmentada (POSER, 2005, p. 35).

Enfim, o grande objetivo é a prática do *marketing* individualizado com foco no cliente, o que além de reduzir os custos do empreendimento empresarial, tende a ser extremamente eficaz.

Como esclarecem alguns autores como Pizzinato e Zem (2005, p. 16), esta estratégia individualizada é o nível mais específico do *Marketing*, uma vez que está concentrado em cada cliente particular, pois as diferenças existentes no comportamento deles exigem das empresas ações muito mais específicas para atender a suas respectivas necessidades e desejos.

Um exemplo concreto de como ocorre esta captura de dados é o sistema dos *cookies*, arquivos que ficam armazenados em determinado computador quando o usuário acessa um site ou clica em uma janela específica, e servem como uma espécie de rastro digital de acessos daquele computador e de seu usuário.

Dessa forma o *cookie* (BORGESIUS, 2014, p. 10)

> [...] é um pequeno arquivo de texto que um editor de sítios na *Internet* armazena no computador ou no smartphone de um usuário para reconhecer aquele dispositivo. [...] Normalmente, esses cookies são relativos à "sessão", pois desaparecem depois que o usuário fecha o navegador. As empresas que atuam na segmentação comportamental costumam usar cookies persistentes para reconhecer os usuários em momentos futuros. Aquelas que publicam anúncios num sítio, como as redes de propaganda, podem colocar e ler também esses cookies persistentes [...] Resulta daí que uma rede de propaganda pode acompanhar o comportamento de um usuário da *Internet* em todos os sítios nos quais ela publica anúncios.

Atualmente a execução do *Marketing* individualizado está facilitada devido aos recursos oferecidos pelas TIC, que possibilitam a gestão estratégica de informações de cada cliente, adotando o *Database Marketing*. Em razão disso, verifica-se que existe uma grande probabilidade de que os internautas sejam vigiados e que seus comportamentos acabem sendo segmentados, sobretudo considerando o fato de que a segmentação feita em bancos de dados é uma prática empresarial extremamente vantajosa para as empresas e altamente estimulada pelas obras sobre *marketing* relacional.

Tal probabilidade decorre de que, em uma sociedade capitalista onde existe um real ganho econômico, as empresas tendem a colocar a vigilância como um valor acima dos direitos humanos e constitucionais que protegem os dados do cidadão internauta.

1.2.2 As influências da Psicologia cognitivo-Comportamental nas práticas empresariais.

Para que seja possível a compreensão das influências psicológicas que a segmentação comportamental submete aos internautas por ela monitorados,torna-se primordial analisar a

tendência da psicologia[30] que explica os efeitos desta atuação empresarial, ou seja, a Psicologia Cognitivo-Comportamental.

E como forma de compreender esta tendência, são essenciais os seguintes passos: o início do estudo deve iniciar-se pela interpretação da Psicologia, após deve haver o estudo das principais correntes de pensamento que fundaram a Psicologia, e, por fim, uma análise das suas atuais tendências no estudo do comportamento humano.

Quando se fala em Psicologia, deve-se considerá-la um conhecimento "poliédrico", pensá-la na forma de um calidoscópio[31].Esta ciência tem um objetivo, está interessada no estudo do comportamento humano, portanto, tem um método próprio e obedece a um rigor científico.

Após todos os movimentos históricos[32] que formaram a Psicologia, é possível identificar na Psicologia atual quatro tendências de pensamento, que correspondem a diferentes metodologias de análise que os profissionais desta área adotam: a psicanalítica[33], a *neobehaviorista*[34], a cognitivista comportamental e a humanista.

A principal característica dos profissionais da segunda tendência é a insistência em fazer perguntas precisas e bem delineadas, utilizando métodos objetivos e realizando pesquisas meticulosas. Tal necessidade, considerando a análise de dados que os sistemas informatizados possibilitam, pode ser uma das principais razões da influência desta forma de Psicologia para a segmentação de dados pessoais.

Assim surge o cognitivismo e "designa-se com esse nome um conjunto de concepções psicológicas cujo objeto principal é o estudo dos processos de aquisição dos conhecimentos e de tratamento da informação" (DORON; PAROT, 2001, p. 150). Tal como uma análise de dados, o cognitivismo "atribui aos comportamentos observáveis um valor de signos cujo estudo permite a inferência de estruturas subjacentes que constituem os verdadeiros objetos dessa psicologia" (DORON; PAROT, 2001, p. 150)

---

[30] Derivada de palavras gregas que significam 'estudo da mente ou da alma'.

[31] Instrumento onde determinada imagem esta constantemente mudando de formato e de cor, utilizado como metáfora do estudo de ciências dinâmicas que estão em constante alteração, como o caso da psicologia.

[32] Esta ciência surgiu historicamente a partir de cinco movimentos filosóficos: o estruturalismo de Wilhelm Wundt, o funcionalismo de William James, o behaviorismo de John Watson, a Psicologia da Gestalt de Max Wertheimer e a psicanalítica de Sigmund Freud (DAVIDOFF, 1983, p. 9-16).

[33] A primeira tendência é a psicanálise, que consiste no ato de retirar conclusões a partir de inferências dos fatos observados, formular hipóteses, compará-las com os fatos posteriores que forem encontrados e, eventualmente, fundir um corpo organizado de material com o fim de verificar a validade das hipóteses (DAVIDOFF, 1983, p. 14).

[34] Os neobehavioristas "investigam os estímulos, as respostas observáveis e a aprendizagem. Também cada vez mais estão estudando fenômenos complicados como o amor, a tensão, a empatia, a confiança e a personalidade." (DAVIDOFF, 1983, p. 19)

E a relação filosófica entre a informática e a tendência cognitivista da Psicologia é claramente apontada por Roland Doron e François Parot (2001, p. 150):

> Reatando com uma tradição filosófica de inspiração racionalista, que considera o pensamento como um cálculo, o cognitivismo estabeleceu uma aliança com a informática, da qual tomou emprestada a maioria de sua metáforas e modelos. Essa atitude levou-o a construir uma correspondência estrita entre as diferentes operações asseguradas pelos componentes fundamentais dos computadores: unidade de controle, unidade de cálculo, memória.

Como visto, os psicólogos desta terceira tendência adotam as seguintes teses (DAVIDOFF, 1983, p. 21): Inicialmente, entendem que devem estudar os processos mentais, tais como o pensamento, a percepção, a memória, a atenção, a resolução de problemas e a linguagem.

Visam à aquisição de conhecimentos precisos sobre como esses processos funcionam e como são aplicados na vida cotidiana, verificando, por exemplo, os acessos e cliques que determinado indivíduo faz em algum site ou o seu tempo de acesso, informações que podem facilmente ser verificadas através do sistema de *cookies*.

Por fim, para a Psicologia cognitiva, deve-se utilizar a introspecção informal, sobretudo para desenvolver intuições, enquanto os métodos objetivos são preferidos para confirmar estas intuições.

Como afirma Judith S. Beck (1997, p. 17-8), a teoria cognitiva, conforme desenvolvida por Aaron Beck, é:

> [...] singular no sentido de que é um sistema de psicoterapia com uma terapia da personalidade e da psicopatologia unificadas, apoiadas, por evidências empíricas substanciais. Ela tem uma terapia operacionalizada com uma ampla gama de aplicações também apoiada por dados empíricos.

O próprio Aron Beck, em obra conjunta com Brad Alford (2000, p. 23), afirma que "[...] a teoria cognitiva da psicopatologia e psicoterapia considera a cognição a chave para os transtornos psicológicos. 'Cognição' é definida como aquela função que envolve deduções sobre nossas experiências e sobre a ocorrência e o controle de eventos futuros."

A tendência da Psicologia cognitiva, também chamada de Cognitiva–Comportamental, é considerada uma:

> [...] abordagem de senso comum que se baseia em dois princípios centrais: 1. Nossas cognições têm uma influência controladora sobre nossas emoções e comportamento; e 2. O modo como agimos ou nos comportamos pode afetar profundamente nossos padrões de pensamento e nossas emoções. (WIGHT; BASCO; THASE, 2008, p. 14)

Os principais elementos do modelo cognitivo Comportamental são: o evento, a avaliação cognitiva, a emoção e o comportamento. Dentre eles, o principal é a avaliação cognitiva, essencial para a compreensão da Segmentação comportamental (WIGHT; BASCO; THASE, 2008, p. 17).

Assim, seguindo as lições de Beck e Alford (2000, p. 21), é possível dizer que

> [...] a teoria cognitiva articula a maneira através da qual os processos cognitivos estão envolvidos na psicopatologia e na psicoterapia efetiva [...] Na teoria cognitiva a natureza e a função do processamento de informação constitui a chave para entender o comportamento mal adaptativo e os processos terapêuticos positivos.

O processamento ou avaliação cognitiva recebe um papel fundamental neste modelo, porque o ser humano continuamente avalia a relevância dos acontecimentos no ambiente que o circunda (por exemplo, eventos estressantes, comentários ou ausência deles, memória de eventos, tarefas a serem feitas, sensações corporais), e estas cognições estão frequentemente associadas a reações emocionais.

Segundo as lições de Beck (1997, p. 21-24), a terapia cognitiva funciona a partir de determinados princípios, pois "se baseia em uma formulação em contínuo desenvolvimento do paciente e de seus problemas cognitivos" – 1º princípio.

Ainda, esta terapia "requer uma aliança cognitiva segura" – 2º princípio, "enfatiza a colaboração e participação ativa" – 3º princípio – é "orientada em meta e focalizada em problemas" – 4º princípio, inicialmente "enfatiza o presente" – 5º princípio.

E "educativa, visa ensinar o paciente a ser seu próprio terapeuta e enfatiza prevenção de recaídas" – 6º princípio, visa "ter um tempo ilimitado" – 7º princípio, as suas "sessões são estruturadas" – 8º princípio, ensina o seu paciente a "identificar, avaliar e responder a seus pensamentos e crenças disfuncionais" – 9º princípio.

E, por fim, "utiliza uma variedade de técnicas para mudar pensamento, humor e comportamento" – 10º princípio.

Na Psicologia cognitiva-Comportamental, estudam-se os chamados pensamentos automáticos, que são:

> [...] cognições que passam rapidamente por nossas mentes quando estamos em meio a situações (ou relembrando acontecimentos). Embora possamos subliminarmente conscientes da presença de pensamentos automáticos, normalmente essas cognições não estão sujeitas a análise racional cuidadosa. [...] Um grande número dos pensamentos que temos a cada dia faz parte de um fluxo de processamento cognitivo que se encontra logo abaixo da superfície da mente totalmente consciente. (WIGHT; BASCO; THASE, 2008, p. 19)

Para a presente dissertação, esta terceira tendência assume grande importância, visto que o *Maketing*, a partir da segmentação comportamental, fundamenta-se basicamente nas teorias cognitivas de impulsos e condicionamentos, e nas noções psicológicas de aprendizagem.

Para uma compreensão de como a segmentação comportamental atinge psicologicamente a subjetividade do indivíduo, sujeito ao *Marketing* Segmentado, é essencial discutir os três métodos que dão forma às reações dos seres humanos: o condicionamento respondante (os reflexos), o condicionamento operante e a aprendizagem por observação.

O condicionamento é um termo empregado para descrever um processo de aprendizagem, "[...] entendida pelos psicólogos *behavioristas* como o processo de aquisição e reprodução de respostas comportamentais específicas sob condições específicas: daí o termo 'condicionamento'." (STRATTON; HAYES, 1994, p. 44)

Importante referir que esses processos fundamentais de aprendizagem[35] (DAVIDOFF, 1983, p. 156) atingem o indivíduo sem que haja uma tentativa deliberada de mudar o seu comportamento. Na maioria dos casos, as pessoas nem percebem que estão submetidas a estes processos.

Conforme esclarecem Roland Doron e François Parot (2001, p. 166), o condicionamento é um:

> Processo de aprendizagem, inicialmente descrito por I. Pavlov, já em 1902, no qual um estímulo chamado condicionante (por exemplo, o tilintar de uma campainha) associado a um estímulo incondicionado (alimento) provoca uma resposta condicionada similar a resposta incondicional (salivação). Mecanismo de aprendizagem associativa posta em evidência por esse processo.

Os chamados respondantes, também conhecidos como reflexos, são eventos desencadeados por outros que lhes são imediatamente antecedentes, sendo que o evento desencadeador é conhecido como estímulo elicitante[36].

Estes respondantes têm características que devem ser analisadas. Inicialmente eles são processos que parecem involuntários, como o som de uma trovoada, que gera uma reação de sobressalto. Ainda, parecem ser controlados pelos eventos que os precedem, ou seja, os

[35] Linda Davidoff (1983, p. 158) esclarece que "a aprendizagem é muitas vezes definida como uma mudança relativamente duradoura no comportamento, induzida pela experiência"

[36] Eventos elicitantes tais como as cócegas, um ruído, um odor, enfim condições espaciais que motivam respostas imediatas, como a gargalhada ou o ato de cobrir os ouvidos ou o nariz.

estímulos elicitantes antes referidos. Por fim, não são apreendidos incialmente, e, portanto, necessitam de certo grau de desenvolvimento do indivíduo em análise.

Além disto, existe um processo de transferência que pode ocorrer quando um destes é transferido de uma situação para outra e ocorre o chamado condicionamento. Tal condicionamento pode ser compreendido com base em determinados elementos de análise (DAVIDOFF, 1983, p. 163).

O primeiro elemento é o estímulo incondicionado (EI), ou seja, aquele estímulo elicitante que ocasiona um respondante automático, e funciona como uma espécie de resposta automática do organismo ao estímulo recebido. Por exemplo, uma comida levada a boca ocasiona o salivamento.

O segundo elemento é a resposta incondicionada (RI), que pode ser definida como o evento, objeto ou experiência que não elicita a resposta incondicionada no início. O estímulo neutro tem que ser combinado com o estímulo incondicionado. Por exemplo, uma campainha que toca todos os dias no horário da refeição pode igualmente ocasionar o salivamento (DAVIDOFF, 1983, p. 163).

O terceiro elemento é o estímulo neutro (EN), que consiste em um evento, objeto ou experiência que não gera no início uma resposta incondicionada. Por exemplo, o som da campainha em princípio não ocasiona o salivamento, portanto este ruído funciona como estímulo neutro.

Por fim, o quarto elemento para a compreensão deste condicionamento respondante é o resultado deste processo, pois após o estímulo neutro ter sido associado ao estímulo incondicionado, este pode vir a evocar uma reação semelhante à resposta incondicionada, denominada resposta condicionada, que, no exemplo citado, seria a situação do salivamento pelo toque da campainha.

Esta estrutura de condicionamento respondante foi desenvolvida por Ivan Petrovick Pavlov, um fisiologista russo, que em seu laboratório fez experiências com animais e constatou que esta associação entre o estímulo neutro e o estímulo incondicionado ocorria com animais que eram alimentados (DORON; PAROT, 2001, p. 166).

Aqui se visualiza o condicionamento operante que consiste em:

> Um processo de aprendizagem estímulo-resposta do comportamento voluntário, que ocorre como um resultado da consequência das ações produzidas pro um organismo animal ou humano. A idéia é de que a aprendizagem de uma consequência de uma ação apropriada ou operante pode ser reforçada – fortalecida – se a ação for seguida de uma consequência agradável. Isso aumenta a probabilidade da ação ocorrer novamente. (STRATTON; HAYES, 1994, p. 45)

Dessa forma era possível a transferência de um estímulo elicitante de determinado respondante para outro, pois era natural o processo de associação.

Ainda, outro processo de aprendizagem que a Psicologia estuda é o condicionamento operante. Linda Davidoff (1983, p. 173) explica que os operantes "são atos iniciados pelos próprios animais. [...] Embora pareçam ser espontâneos e estarem inteiramente sob o controle do animal, os operantes são influenciados por suas competências".

O operante, assim como o conceito estudado anteriormente, está sujeito a um processo de condicionamento denominado condicionamento operante (ou instrumental), que ocorre quando as consequências que se seguem a uma operante aumentam ou reduzem a probabilidade de que esse operante seja realizado em situação semelhante, assim (DAVIDOFF, 1983, p. 174):

> Durante um condicionamento operante a frequência de um ato (o operante) é modificada. Se um dado operante for repetidamente acompanhada de resultados agradáveis para o sujeito, o ato rem probabilidade de ser repetido menos frequentemente em circunstâncias correspondentes. Através da nossa vida cotidiana há constantemente operantes sendo condicionados, em geral sem que disso tenhamos consciência

Os condicionantes operantes foram trabalhados por Burrhus Frederic Skinner, psicólogo norte-americano, que, estudando o comportamento de ratos de laboratório e pombos, identificou que eles poderiam aprender a pressionar um determinado botão se recebessem uma recompensa por aquele ato, e, portanto, mesmo sem qualquer raciocínio mais elaborado, poderiam ser condicionados a determinada atitude.

Operante é um:

> Termo introduzido por B.F. Skinner, para designar uma forma de condicionamento distinta, segundo ele, do condicionamento pavloviano, ou respondente. O condicionamento operante é essencialmente caracterizado pela ligação entre uma resposta operante e o reforço, sendo a primeira a condição do segundo.(DORON; PAROT, 2001, p. 554)

Dentro da questão do condicionamento operante, é possível identificar aquilo que na Psicologia denomina-se "*biofeedback*", que decorreu do termo "*feedback*", desenvolvido pelo matemático Norbert Weiner (*apud* DAVIDOFF, 1983, p. 163), que significa o "método de controlar um sistema, reinserindo nele os resultados de seu desempenho anterior".

No caso, o "*biofeedback*" significa uma forma de ensinar os indivíduos a controlar os processos corporais, fornecendo uma informação sistemática sobre o que uma determinada

parte está fazendo, sendo esta técnica utilizada no tratamento de diversos tipos de enfermidades.

Pode-se dizer que “a terapia cognitiva baseia-se no *modelo cognitivo*, que levanta a hipótese de que as emoções e comportamentos das pessoas são influenciadas por sua percepção dos eventos” (BECK, 1997, p. 29).

Como esclarece Judith T. Beck (1997, p. 29) “O modo como às pessoas se sentem está associado ao modo como elas interpretam e pensam sobre uma situação. A situação em si não determina diretamente como elas se sentem; sua resposta emocional é intermediada por sua percepção da situação.”

Por fim, o terceiro processo de aprendizagem é denominado pela Psicologia de aprendizagem por observação, e ocorre quando o comportamento de um indivíduo muda de modo permanente como resultado da observação dos atos de outros indivíduos.

Esta aprendizagem por observação ocorre a partir dos seguintes processos: em primeiro lugar, a aquisição que ocorre quando o indivíduo observa um modelo que se comporta de determinado modo e reconhece os traços distintivos da conduta do modelo; em segundo lugar, a retenção que ocorre quando a atividade do modelo é armazenada ativamente na memória do indivíduo observador; em terceiro lugar, o desempenho que se manifesta quando o indivíduo analisa se o comportamento do modelo observado tende a levar a consequências positivas é suscetível de ser reproduzido; por fim, as consequências que ocorrem quando o indivíduo se defronta com os efeitos da reprodução do comportamento do modelo, ocorrendo então o condicionamento operante.

Linda Davidoff (1983, p. 202) afirma que:

> a aprendizagem por observação é muito mais complicada do que o condicionamento operante ou o respondante. Observe que sempre implica atividades cognitivas e costuma ser também muito demorada. Como o condicionamento operante e respondante, a aprendizagem por observação pode ser usada deliberadamente na modificação do comportamento.

Dessa forma, é possível identificar que a segmentação comportamental e as estratégias de *Marketing* que nela são baseadas psicologicamente estão fundamentadas na teoria cognitiva Comportamental, onde as técnicas de aprendizagem estudadas atuam inconscientemente sobre os internautas submetidos a estas estratégias.

O condicionamento respondante ocorre em situações como quando determinado anuncio é enviado a determinado indivíduo em um momento específico em que este anúncio serviria como um estímulo elicitante a um ato inconsciente de aquisição de determinada

mercadoria ou contratação de algum determinado serviço. Por exemplo, um site que possibilite ao indivíduo ter conhecimento do valor líquido que receberá de seu salário, descontados os encargos sociais, ao anunciar determinado produto que este indivíduo tenha anteriormente acessado, pode funcionar como um motivador para uma aquisição não consciente.

Ou ainda, este *Marketing* Segmentado pode ocasionar um condicionamento operante, quando, por exemplo, durante um processo de compra em algum determinado site, o sistema possibilite ao indivíduo realizar a compra de outros produtos que não escolheu inicialmente, mas que podem ser de seu interesse em vista daquilo que ele está adquirindo, simplesmente anexando estes produtos ao seu pedido. Algo que pode trazer vantagens, mas que de certa forma pode motivá-lo a agir de forma inconsciente, apenas clicando em determinada ferramenta.

Por fim, a aprendizagem por observação também ocorre com o *Marketing* Segmentado naquelas situações em que os sites indicam, por exemplo, que as pessoas que adquiriram determinado produto também adquiriram outros semelhantes, ou mesmo quando os sites possibilitam a avaliação de determinados produtos ou serviços, o que pode induzir pela observação a aquisição ou contratação.

Realmente aqui também há uma vantagem, pois possibilita ao indivíduo conhecer o que outras pessoas adquiriram e o que pensam sobre determinados produtos. Porém, quando alguns destes avaliadores tornam-se personalidades respeitadas em determinados segmentos – como no caso de jovens que criam blog de beleza e anunciam produtos cosméticos de determinadas marcas – questiona-se qual a responsabilidade destas pessoas pelos produtos que elas afirmam utilizar e avaliam positivamente.

Como esclarece Paula Sibila (2008, p. 23):

> Já neste século XXI que está ainda começando, as "personalidades" são convocadas a se mostrarem. A privatização dos espaços públicos é outra face de uma crescente publicização do privado, um solavanco capaz de fazer tremer aquela diferenciação outrora fundamental. Em meio a vertiginosos processos de globalização dos mercados em uma sociedade altamente midiatizada, fascinada pela incitação à visibilidade e pelo império das celebridades, percebe-se um deslocamento daquela subjetividade "interiorizada" em direção a novas formas de autoconstrução.

A autora continua afirmando que a exibição da intimidade e a espetacularização da personalidade são duas faces de um mesmo fenômeno que denota um deslocamento dos eixos em torno dos quais as subjetividades modernas se construíram. Assim, desloca-se a estrutura

do eu para o exterior, abandonando o lócus interior gradativamente, incitando os indivíduos a se mostrarem. (SIBILA, 2008, p. 115).

Da mesma forma, André Lemos (2002, p. 12) afirma:

> A vida comum transforma-se em algo espetacular, compartilhada por milhões de olhos potenciais. E não se trata de nenhum evento emocionante. Não há histórias, aventuras, enredos complexos ou desfechos maravilhosos. Na realidade, nada acontece, a não ser a vida banal, elevada ao estado de arte pura. A vida privada, revelada pelas webcams e diários pessoais, é transformada em um espetáculo para olhos curiosos, e este espetáculo é a vida vivida na sua banalidade radical.

Contudo, como as empresas adotam estas práticas e as direcionam a determinados indivíduos? Como elas identificam aqueles indivíduos que estariam vulneráveis a estas técnicas psicológicas?

A resposta é clara: isso ocorre com base nos bancos de dados pessoais que os internautas fornecem ao acessar os sistemas informatizados quando utilizam das tecnologias informacionais e comunicacionais (TIC).

Neste ponto surgem os denominados "dossiês digitais",que serão estudados no próximo ponto e possibilitarão uma compreensão de como estas técnicas podem ser utilizadas.

1.2.3 A vulnerabilidade dos dados pessoais em face da segmentação comportamental.

As TIC – computadores e *Internet* – viabilizam a coleta, o processamento e a utilização de informações pessoais, para fins específicos, a ponto de permitir que o nome de determinado indivíduo seja impresso em uma oferta individualizada e remetida para a sua residência, e isso poderá ocorrer com milhões de pessoas que o sistema considerar parte do mesmo nicho social.

Tradicionalmente a estrutura de proteção da privacidade, da vida privada e da intimidade, como esferas circunscritas de proteção, contribui para a manutenção deste *status quo*, no sentido de que a violação à personalidade individual aparentemente pode ser justificada com base no fato de que não se adentrou em determinada esfera. Convencionalmente a privacidade foi pensada a partir da denominada "teoria da pessoa como uma casca de cebola"[37]. Tal teoria entendia que as noções de intimidade, vida privada e vida

[37] Como esclarece o Danilo Doneda (2006, p. 67) esta doutrina: "de Hubmann, constantemente referida, que utiliza um esquema de esferas concêntricas para representar os diferentes graus do sentimento de privacidade: a esfera da intimidade ou do segredo [...] a esfera privada [...] e, em torno delas, a esfera pessoal, que abrangia a vida pública [...]. Tal teoria que hoje chega a ser referida pela doutrina alemã como a teoria da 'pessoa como uma cebola passiva', foi desenvolvida e posteriormente abandonada (em célebre sentença de 1983), pelo Tribunal Constitucional Alemão."

pública eram círculos concêntricos e distintos, onde a violação seria mais grave quanto mais atingisse a menor das esferas.

Porém essa visão atualmente tem sido abandonada em favor de um tratamento mais unitário de tal direito, como afirma Pérez Luño (2005, p. 338-9):

> O reconhecimento das diferentes formas de agressão à intimidade, a imagem e a honra, não podem de modo algum, reduzir a importância do caráter unitário da estrutura deste direito [...]A doutrina tradicional havia traçado determinados critérios de distinção entre os direitos a honra, a fama e a reputação, considerados como um interesse próprio da vida nas relações sociais, e o direito a intimidade, entendido como aspiração do indivíduo a tranquilidade do espirito e ao isolamento. Porém as dificuldades que este esquema diferenciador põem em evidência quando se adverte que: De um lado a definição de honra junto a sua dimensão externa consiste em uma consagração social, em reconhecimento que os outros lhe outorgam ou tributam, possui uma dimensão íntima de 'patrimônio da alma', que afeta o âmbito mais interno da personalidade e o mais próprio e intransferível do indivíduo, e de outro, que a intimidade, tal como se tem estudado, para além de uma possibilidade de isolamento implica um direito de participação e de controle das informações que concernem a cada pessoa.

Desta forma, não é possível compreender a estrutura da intimidade, da vida privada ou da privacidade de forma independente – ou na forma de círculos concêntricos. Tanto por que a estrutura externa de proteção da privacidade carrega um conteúdo de personalidade interna e, portanto, de intimidade, como pelo fato de que a intimidade atualmente, sobretudo tendo em conta as violações que o avanço das TIC e pode ocasionar, também pode ter um conteúdo externo de proteção e controle sobre informações íntimas, uma autodeterminação informativa.

Como forma de superar esta estrutura em esferas de proteção, surgiram diversas outras construções teóricas que pretendem possibilitar a proteção da personalidade individual. Dentre elas, uma estrutura interessante é a construção partir da ideia de um "mosaico", que se adequa a sociedade informacional, onde o elemento mais importante é o uso que será feito dos dados coletados.

Com base na teoria de Fulgência Madrid Conesa, Marcel Leonardi (2012, p. 74) pondera – considerando que na sociedade informacional os espaços público e privado são relativos – que a forma de proteção deve ser analisada em função de quem é o outro sujeito em uma 'relação informativa'.

Existem dados irrelevantes do ponto de vista da personalidade individual quando isolados, mas que em conexão com outros, talvez igualmente irrelevantes quando isoladamente considerados, podem servir para tornar totalmente transparente a personalidade de um indivíduo através do cruzamento desses dados.

Outro autor também citado por Leonardi (2012, p. 74) é Daniel J. Solove, que estuda a criação dos chamados ‘dossiês digitais’ a partir do fluxo de informações entre bancos de dados e cadastros mantidos por entidades privadas, governos e indivíduos.

Enfim, a principal consequência a ser evitada com a regulamentação destes “dossiês digitais” – surgidos da combinação de dados pessoais e que possibilitam a criação de um perfil do Internauta – é que eles possibilitem a prática de “*Datavigilance*”.

As informações fornecidas pelas pessoas para que obtenham determinados serviços são tais, em quantidade e qualidade, que possibilitam uma série de usos secundários, especialmente lucrativos para os gestores dos sistemas interativos (RODOTÁ, 2008, p. 46).

Estes gestores armazenando, filtrando e segmentado as informações obtidas quando do fornecimento dos serviços, podem ‘criar’ informações novas (perfis de consumo individual e familiar, análises de preferência, informações estatísticas, etc.), que interessam a outros sujeitos, a quem estas informações podem ser vendidas. Por isso, torna-se difícil individualizar algum tipo de informação da qual o cidadão poderia ‘despir-se’ completamente (RODOTÁ, 2008, p. 36), no sentido de renunciar definitivamente ao controle das modalidades de seu tratamento e das atividades dos sujeitos que as utilizam. Isto decorre da percepção de que até mesmo as informações aparentemente inócuas podem, integradas a outras, provocar dano ao interessado.

Efetivo exemplo de captação de dados que possibilita violações à personalidade do indivíduo – através da combinação destes – é o sistema da empresa Google, como afirma Siva Vidhyanathan (2011, p. 98):

> Quanto mais o GOOGLE souber sobre nós, mais eficientes serão seus serviços de propaganda. Entender a natureza desse armazenamento de perfis e da segmentação do consumidor é o primeiro passo para entender a googlelização de nós. [...] Nossa fé cega no Google deu à empresa condições de afirmar que oferece aos usuários um controle substancial sobre o modo como suas ações e preferências são coletadas e utilizadas.

E conclui (2011, p. 113) afirmando que “A vigilância maciça está presente na vida humana desde o século XVIII. As ferramentas digitais simplesmente tornaram mais fácil coletar, misturar e vender bases de dados.”

Paul Virilio (1999, p. 61) esclarece que a questão da autoexposição na atual sociedade tem uma explicação psicológica: “Com esse *voyeurismo,* a tele vigilância adquire um novo sentido: não se trata mais de se prevenir contra uma intrusão criminosa, mas de partilhar suas angústias, seus fantasmas, com toda uma rede, graças á superexposição de um lugar da vida”.

Como afirma Paula Sibila (*in* LEMOS; CUNHA, 2003, p. 150):

> As possibilidades inauguradas pelos meios eletrônicos como a *Internet*, que permitem a "qualquer um" ser visto, lido ou ouvido por milhões de pessoas – mesmo que não se tenha nada específico a dizer – talvez esteja dando conta dessa falta de sentido que marca as experiências subjetivas contemporâneas: uma carência que consegue dotar de valor ao mero fato de se exibir, de ser *visível* mesmo que seja na fugacidade de um instante de luz virtual.

Afinal, essa relação de confiança/captação de dados com estas empresas não é regulamentada por meio de um contrato? Portanto, não haveria o exercício de uma liberalidade por parte do usuário que solicita os serviços destes entes e, em contrapartida, disponibiliza seus dados?

Sim, há uma atuação voluntária do indivíduo ao disponibilizar seus dados pessoais a estas empresas e a vontade do indivíduo no exercício do direito à intimidade tem um papel decisivo e incontestável, pois o interessado pode livremente optar por deixar de exercer o seu direito, ou ainda decidir em que medida exercê-lo.

Todavia, adverte Keiko Mori (2002, p. 56), esta disposição de vontade no ambiente virtual, dentre outras questões essenciais, encontra solução na diferença de caráter temporal, ou seja, no caso do consentimento do interessado (no ambiente físico), o indivíduo opta por temporariamente deixar de exercer o seu direito, enquanto a renúncia (como ocorre com os dados virtuais, que podem ficar praticamente acessíveis para toda a eternidade) é duradoura, e, portanto, inaceitável.

Além desta concessão perpétua para a utilização dos dados, ainda ocorre a perda da autodeterminação informativa, pois o internauta que fornece os seus dados perde completamente a possibilidade de controlar a utilização que é feita destes dados.

Dessa forma, considerando que os dados pessoais armazenados em sistemas informacionais podem ser mantidos por longos períodos de tempo, inclusive por toda a vida do titular destes dados e mesmo posterior a sua morte, a liberalidade consistiria em uma verdadeira renúncia ao direito fundamental.

Ainda há de se considerar que o cidadão, em regra, é incapaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados (RODOTÁ, 2008, p. 37). Como forma de evitar este tipo de alegação de que o indivíduo cede voluntariamente os seus dados pessoais e que, portanto, a utilização destes dados pela empresa que recebe estas informações teria sido consentida no momento da contratação, desenvolveu-se uma nova forma de garantia, a "autodeterminação informativa".

Da contraposição existente entre a proteção de dados e a informática surge a autodeterminação informativa (LIMBERGER, 2007, p. 232), e através dela o indivíduo estabelece os limites das invasões das tecnologias informacionais na sua personalidade.

Como esclarece Pérez Luño (2005, p. 336), baseado-se na estrutura concebida por Georg Jellinek:

> [...] em nossa época resulta insuficiente conceber a intimidade como um direito garantia (*status* negativo) de defesa frente a qualquer invasão indevida a esfera privada, sem contemplá-la, ao mesmo tempo, como um direito ativo de controle (*status* positivo) sobre o fluxo de informações que afetam cada sujeito.

Com isso, verifica-se que a autodeterminação constitui-se em uma garantia de proteção à personalidade do indivíduo internauta na sociedade informatizada. Nesse contexto, a autodeterminação caracteriza-se como uma garantia de que o titular de determinado dado deverá ter um conhecimento razoável sobre as utilizações que serão feitas por tal informação.

Esta ampliação de conteúdo do valor intimidade tem ocasionado uma reconstrução do seu significado e da sua carga valorativa e, dessa forma:

> Em nossos dias, junto a sua conexão tradicional, já comentada com o valor dignidade, identifica-se a intimidade com a própria noção de liberdade, pois ela define as possibilidades reais de autonomia e de participação na sociedade contemporânea; inclusive quando concebida como faculdade de controle das informações que lhes concernem por parte dos indivíduos e dos grupos, aparece como uma condição para uma convivência política democrática, que se confunde com a defesa da igualdade de direitos. (PEREZ LUÑO, 2005, p. 336)

Assim, passa-se a identificar um direito específico, decorrente da privacidade na "proteção dos dados pessoais (sejam íntimos ou não íntimos) frente aos tratamentos informáticos e telemáticos, o que a doutrina ora denomina autodeterminação informativa, ora liberdade informática." (PEREIRA, 2005, p. 145).

Dessa forma, verifica-se que é essencial uma releitura do direito à proteção da personalidade dentro da perspectiva informacional, como forma de possibilitar o desenvolvimento de novos mecanismos de proteção e manutenção da "autonomia informativa".

Essa 'autonomia informativa' (PEREIRA, 2005) refere-se a um direito emergente, que veio para ampliar a proteção à personalidade individual e que, em conjunto com outros direitos (como o direito à proteção dos dados pessoais), passou a fazer parte do rol de direitos fundamentais constitucionalmente consagrados, os quais possuem, como escopo comum, a proteção da dignidade da pessoa humana.

A *Internet* (KAKU, 2000, p. 87) está sendo dominada pelo comércio, e isso tem ocorrido com insuficiente regulação, o que permite às empresas agir unicamente voltadas para seus interesses econômicos, possibilitando a violação da privacidade dos usuários, que, por sua vez, tornam-se práticas normais do comércio.

Dessa forma, os bancos de dados tornam-se um atrativo para o comércio em geral por sua facilidade de obtenção e pela possibilidade de condicionarem as decisões empresariais na busca do máximo lucro. Assim, a obtenção de tais informações permite o manuseio fácil e barato dos dados, com a finalidade de traçar estratégias que possam favorecer os negócios de quem a obtiver (KAKU, 2000, p. 89).

Com muita frequência, percebe-se a rápida obsolescência das soluções jurídicas que se referem a um único e isolado problema que envolva questões tecnológicas. Portanto, adverte-se para a necessidade de individualizar princípios e de associá-los a tendências de longo prazo como forma de instrumentalizar a atuação dos juristas na solução destas questões (RODOTÁ, 2008, p. 42).

No início das discussões sobre os riscos para a privacidade, as primeiras hipóteses legislativas sobre a proteção das informações pessoais faziam referência a uma realidade tecnológica na qual os computadores que então estavam em operação – na qual o funcionamento se inspirava a leitura do problema – equivaliam em sua potência de cálculo aos atuais computadores pessoais (RODOTÁ, 2008, p. 43).

Atualmente se tornaram inutilizáveis as definições legislativas concebidas com vistas a sistemas informáticos construídos em torno dos grandes computadores, os chamados "*Mainframes*". Como exemplo desta inutilização, Stéfano Rodotá (2008, p. 43) refere-seà questão da definição de arquivo de dados pessoais, na Lei Sueca de 1998, como 'registro obtido mediante um sistema de elaboração automática de dados que contém dados pessoais referentes à pessoa interessada'.

Tal definição não pode mais ser usada para fundamentar obrigações comuns a todos os que criam e administram arquivos deste gênero, sob pena de tornar-se inócua, pois abarcaria como gestor de dados todo aquele proprietário de um computador pessoal. Não é que haja necessariamente uma lacuna jurídica, mas, como afirma Patrícia Peck (2002, p. 37),"[...] há, sim, falta de entendimento quanto à aplicação de leis em vigor para questões relativamente novas, que exigem interpretação da norma e sua adequação ao caso concreto".

Conforme será visto no segundo subcapítulo do capítulo seguinte, existem legislações em muitos países que regulamentam a proteção de dados pessoais. Contudo, a grande complexidade surge na (in) capacidade técnica dos aplicadores destas legislações de

compreender a nova realidade de uma sociedade profundamente alterada pela massiva utilização das TIC.

Além disso, como será analisado no terceiro subcapítulo do capítulo seguinte, muitas vezes observa-se a falta de vontade das empresas em aplicar as previsões das legislações que buscam regulamentar tal questão. Tal constatação ocorrerá a partir das previsões dos termos de política de privacidade que elas disponibilizam aos seus usuários, o que será feito na última parte desta dissertação.

2 O TRATAMENTO JURÍDICO DOS DADOS PESSOAIS NA *INTERNET* E OS DEVERES DE CONFIANÇA E INFORMAÇÃO.

O capítulo anterior teve por objetivo construir o significado da segmentação comportamental através dos dados pessoais registrados em arquivos digitais, estabelecer as suas diretrizes teóricas, bem como identificar, com base em outras áreas do conhecimento tais como a Psicologia e o *Marketing*, as causas e consequências de sua ocorrência.

Este capítulo inicial também teve por objetivo construir a perpectiva teórica da proteção de dados pessoais a partir da autoderteminação informativa como um novo meio de proteção da privacidade do indivíduo que se utiliza das tecnologias informacionais e comunicacionais e sua vulnerabilidade em face da vigilância massiva dos indivíduos.

Tanto o avanço da proteção de dados pessoais como o risco de excessiva vigilância foram identificados como cenários onde o fenômeno da segmentação comportamental com base em dados pessoais ocorre.

Neste segundo capítulo, tem-se o propósito de apresentar formas de como juridicamente evitá-la ou ao menos regulamentá-la, e este objetivo será feito através da identificação e comparação de diferentes experiências legislativas.

Optou-se por realizar uma comparação entre as legislações específicas de dois países latino-americanos e as previsões até então existentes no ordenamento jurídico brasileiro sobre a temática da proteção de dados pessoais na *Internet*. A escolha destes países justificou-se pelo fato de que ambos foram declarados como tendo uma proteção de dados adequada para os padrões da União Européia, considerando que a idéia de proteção de dados pessoais surgiu dentro daquele bloco de nações.

Porém, somente o estudo comparativo das legislações não seria capaz de possibilitar a verificação da eficácia destas experiências para a redução da prática ilícita da segmentação comportamental, ou ao menos para vinculá-la à vontade do titular dos dados pessoais, tornando-a lícita e protegendo o indivíduo submetido a estas práticas.

Desta forma optou-se por buscar identificar como um intermediário específico de acesso à *Internet*, o provedor de acesso, declara o tratamento que dará aos dados pessoais. Dentre os provedores, optou-se pelo “Terra”, considerando ser um dos maiores portais de serviços de *Internet* do Brasil, que também funciona como um provedor de acesso, e que, por sua vez, funciona como um portal de conteúdo, vinculado a provedores de acesso nos países estudados.

Após o estudo comparativo das legislações de proteção de dados pessoais da Argentina, do Uruguai e do Brasil, haverá uma análise dos Termos de Privacidade do Portal Terra no Brasil e na Argentina, visto que o portal argentino também é veiculado no Uruguai, e oferece todos os serviços vinculados a esta marca específica, dentre os quais os provedores de acesso.

Registre-se que os termos de política de privacidade não são documentos bilaterais[38], constituindo-se em espécie de manifestação de intenções do portal, concretizados em um documento unilateral, mas que deve comprometer a atuação deste provedor – e dos serviços a ele vinculados – a partir da noção de boa-fé objetiva.

Portanto, é essencial compreender como esta noção contratual é capaz de vincular o portal a cumprir as previsões do seu termo de política de privacidade e, assim, justificar como efetivamente a concretização da ideia de proteção de dados, a partir das previsões dos termos, irá ocorrer nos países analisados.

2.1 A BOA-FÉ OBJETIVA NAS RELAÇÕES COM OS PROVEDORES DE ACESSO À *INTERNET*: ANÁLISE DE TERMOS DE POLÍTICA DE PRIVACIDADE.

Os provedores de serviços de *Internet* – como é o caso dos provedores de acesso, conteúdos, etc. – são prestadores de serviço que têm sua relação com o usuário regulamentada por um contrato onde precisamente constam as obrigações, seja disponibilização de um conteúdo, seja acesso à rede mundial de computadores (*Internet*), entre outras finalidades que será remunerado por um valor contratado.

Além disto, para esta prestação se efetive é essencial que o usuário seja corretamente identificado. Portanto, exige-se a disponibilização de dados pessoais, a qual geralmente aparece nos contratos de prestação de serviços como uma obrigação do usuário. Porém estes contratos não preveem a forma e a finalidade de utilização destes dados, ou seja, se servirão apenas para identificar o usuário que utilizará o serviço, ou para outros objetivos não declarados.

Como a proteção aos dados pessoais cada vez mais aparece como uma releitura e um aprofundamento de um Direito fundamental à privacidade, as empresas acabaram por demonstrar o seu intuito de proteger estes direitos através de documentos unilateralmente produzidos e disponibilizados, denominados Termos de Política de Privacidade.

[38] Inclusive os próprios contratos de prestação de serviços são considerados "contratos de adesão", onde não há uma construção bilateral das condições pacutadas por partes em situação equivalente.

Para além da denominação, é possível juridicamente exigir que os provedores de acesso à *Internet* cumpram o que determinam os seus Termos de Política de Privacidade, considerando que eles não estão incluídos como objeto principal da contratação de tal serviço? Ou ainda, qual é o papel destes documentos, considerando tratarem-se de instrumentos de autorregulação estabelecidos pelas próprias empresas?

A resposta para estes questionamentos passa necessariamente pela compreensão do Direito Civil a partir de uma abordagem constitucionalizada, isto é, uma forma de interpretação dos atos e negócios jurídicos – para além de uma visão meramente privatística – que atente para a realidade constitucional. Esta visão exige a compreensão daquilo que muitos autores[39] denominam de "direito civil-constitucional".

Esta forma de visualizar o Direito Civil retira o foco de atenção do próprio Código, centrando a interpretação a partir das escolhas políticas, princípios, direitos e garantias previstas na Constituição Federal. Uma constituição, em um Estado Democrático de Direito, para que tenha de fato força normativa, deve pautar e disciplinar a interpretação da realidade jurídica e política de sua sociedade.

A idéia de força normativa foi pensada inicialmente por Konrad Hesse (1991, p. 24), e sintetizada de modo a comprovar que a Constituição jurídica está condicionada pela realidade concreta do seu tempo. Porém, a pretensão de eficácia da Constituição jurídica não configura apenas a expressão de uma dada realidade, pois devido ao elemento normativo, ela também ordena e conforma a realidade política e social.

As possibilidades, mas também os limites da força normativa, resultam da correlação entre ser e dever ser. Assim, a Constituição logra conferir forma e modificar a realidade, despertando "a força que reside na natureza das coisas", tornando-a ativa. Desse modo, ela própria se converte em força ativa que influi e determina a realidade política e social.

No caso dos Direitos de Personalidade, esta visão e força normativa colocam no centro do sistema o princípio fundamental da dignidade da pessoa humana. **C**omo afirma Barroso (2009, p. 369), este princípio "promove uma despatrimonialização e uma repersonalização do direito civil, com ênfase em valores existenciais e do espírito, bem como o reconhecimento e desenvolvimento dos direitos da personalidade, tanto na sua dimensão física como psíquica".

Dentre os princípios gerais previstos constitucionalmente e decorrentes deste princípio fundamental, está a idéia de boa-fé objetiva, significando aquelas regras de comportamento

[39] Dentre os autores que seguem esta tendência é possível citar Gustavo Tepedino (2001), Paulo Luiz Lôbo Neto (2003) e Judith Martins Costa (2000), dentre outros.

referentes à eticidade, probidade, informação, que surgem antes, durante e mesmo após qualquer negócio jurídico, para além da tradicional visão da boa-fé subjetiva.

Como esclarece Judith Martins Costa (2000, p. 411), "A expressão 'boa-fé subjetiva' denota estado de consciência, ou convencimento individual de obrar [a parte] em conformidade ao direito [sendo] aplicável, em regra, ao campo dos direitos reais, especialmente em matéria possessória".

Por outro lado, a boa-fé objetiva significa "modelo de conduta social, arquétipo ou *standart* jurídico, segundo o qual cada pessoa deve ajustar sua conduta a este arquétipo, obrando como obraria um homem reto: com honestidade, lealdade, probidade" (MARTINS-COSTA, 2000, p. 411).

Esta visão de boa-fé objetiva como um princípio capaz de criar deveres que não necessariamente decorrem do negócio jurídico ou da contratação, objeto principal da relação jurídica, foi primeiramente pensada por Clóvis do Couto e Silva na clássica obra "A obrigação como um processo".

Até esta obra, o pensamento majoritário da doutrina visualizava a existência da boa-fé como princípio geral de qualquer negócio jurídico. Porém a grande inovação foi que antes dela "[...] os autores que, no Brasil, versaram a matéria não procuraram visualizar a boa-fé como elemento criador de novos deveres dentro da relação obrigacional, deveres – convém frisar – que podem nascer e desenvolver-se independentemente da vontade." (SILVA, 2006, p. 35)

Como esclarece Joaquim de Sousa Ribeiro (2003, p. 147):

> Na cultura jurídica continental, e em particular na germanista, a boa-fé tem, como é sabido, uma enorme amplitude e diversidade aplicativas, não regulando apenas a interpretação e execução de um contrato validamente constituído, com vista à cabal realização dos seus fins. A boa-fé é também fonte de deveres de conduta em todas as fases da vida da relação. E da observância desses deveres pode depender, entre outras consequências, a eficácia vinculativa do contrato.

Antes desta nova construção doutrinária, a idéia de boa-fé era uma preocupação adstrita a temas envolvendo direitos reais, o que decorria naturalmente da visão eminentemente patrimonialista que o direito privado da época estava impregnado. Porém nas relações obrigacionais, esta visão de possibilidade de surgimento de deveres decorrente das legítimas expectativas de comportamento "[...] se operou em grande parte, de forma não conscientizada, sob o manto da interpretação integradora ou da 'construção' jurisprudencial." (SILVA, 2006, p. 35).

Como a grande maioria dos princípios normativos, a boa fé acaba por produzir efeitos nos mais diversos contextos e situações e "a sua exigência básica e geral de conduta correta e leal, ramifica-se em normas de conduta mais particularizadas, moldadas pela configuração e valoração dos interesses em jogo em cada domínio." (RIBEIRO, 2003, p. 147)

Até a visão da obrigação como um processo dinâmico que deve ser interpretado a partir de sua totalidade concreta, a manifestação de vontade era o grande paradigma que estabelecia os deveres e obrigações decorrentes de um negócio jurídico. No caso do presente tema, a base do relacionamento entre usuário e provedor de acesso seria o contrato estabelecido entre as partes. Porém o sistema jurídico afasta-se do modelo tradicional do direito das obrigações, fundado na valorização jurídica da vontade humana, e caminha no sentido de inaugurar um novo paradigma para o direito obrigacional, não mais baseado exclusivamente no dogma da vontade, mas na boa-fé objetiva. (MARTINS-COSTA, 2000, p.394)

Ou como esclarece Clóvis do Couto e Silva (2006, p. 36):

> Por meio da interpretação da vontade é possível integrar o conteúdo do negócio jurídico com outros deveres que não emergem diretamente da declaração. Em muitos casos, é difícil determinar, com firmeza, o que é resultado da aplicação do princípio da boa-fé e o que é conquista da interpretação integradora. Além disto, o princípio da boa-fé revela-se como delineador do campo a ser preenchido pela interpretação integradora, pois, de perquirições dos propósitos e intenções dos contratantes, pode manifestar-se a contrariedade do ato aos bons costumes ou à boa-fé[40].

O Termo de Política de Privacidade, mesmo não emanando necessariamente da vontade de ambas as partes, passa a integrar o referido negócio jurídico, pelo menos em face da entidade que o disponibiliza, pois representa uma série de deveres que decorrem da interpretação da vontade das partes e outros que são exigência das normas de conduta, como eticidade, probidade e informação.

Assim, a categoria de deveres que passa a ter grande importância é a dos denominados secundários, anexos ou instrumentais (SILVA, 2006, p. 91), sobretudo quando se trata de documentos que não necessariamente decorrem do instrumento contratual, mas dos

[40] Silva (2006, p. 38) explica que: "A prestação principal do negócio jurídico é determinada pela vontade. Para que a finalidade do negócio seja atingida, é necessário que o devedor realize certos atos preparatórios, destinados a satisfazer a pretensão do credor. [...] Outros, porém surgem desvinculados da vontade, núcleo do negócio jurídico, por vezes ligados aos deveres principais e deles dependentes, por vezes, possuindo vida autônoma. Os deveres desta ultima categoria, chamados independentes, podem perdurar mesmo depois de adimplida a obrigação principal"

comportamentos consistentes em expectivas legítimas de qualquer contratante, como é o caso dos referidos Termos de Política de Privacidade.

A relação jurídica foi tradicionalmente estabelecida a partir de determinados elementos externos – sujeitos, objeto, vínculo jurídico, fonte deste vínculo – e cada espécie de contratação passou a contar com estes elementos. Porém, para além deste aspecto externo, é necessário compreender um aspecto interno.

Para uma melhor compreensão é essencial garantir que esta relação também seja integrada por fatores e circunstâncias que não necessariamente decorrem do estabelecido na legislação ou que emanem da manifestação de vontade, "mas, por igual, fatores extravoluntarísticos, atinentes a concreção de princípios e *standart* de cunho social e constitucional." (MARTINS-COSTA, 2000, p.394)

O significado desses elementos internos está intimamente relacionado aos deveres de informação. Estes deveres consistem na exigência de que o sujeito da relação obrigacional – no presente caso, o provedor de acesso – forneça de forma clara, direta e verdadeira todas as informações pertinentes ao negócio jurídico estabelecido entre as partes – os termos de política de privacidade.

Obviamente não é possível tipificar exaustivamente o conteúdo destes deveres (MARTINS-COSTA, 2000, p.395), determinar, abstrata e aprioristicamente a situação em que os mesmos se revelam, sua intensidade – que variará, por exemplo, quer se trate de uma relação em que as partes são fundamentalmente desiguais, quer se trate de uma relação substancialmente paritária.

Paulo Nalin (1998, p. 190) entende que:

> Tomando como vértice da dignidade do homem, este sim como valor (princípio) fundamental da ordem constitucional, se não diretamente elevada aquela esfera superior, parece produzir a boa-fé algum reflexo de cunho constitucional, enquanto realizador, o princípio da boa-fé para a execução do contrato, da justiça social, e *in casu*, da justiça contratual.

Como decorrência desta justiça contratual, surgem os *deveres de informação* que têm mesma fonte mediata (respeito da ordem jurídica estabelecida entre todos os cidadãos) que os deveres tradicionalmente decorrentes da vontade, porém não têm a mesma fonte imediata – boa-fé objetiva e não declaração da vontade.

Assim, após a incidência da "boa-fé objetiva" nas relações jurídicas obrigacionais, sobretudo vistas como uma totalidade, um processo, percebe-se a agregação aos deveres

contratuais propriamente ditos de outros deveres, que serão denominados instrumentais ou funcionais. (MARTINS-COSTA, 2000, p.403)

Estes deveres funcionais, no caso os *deveres de informação*,"derivam dos princípios e da função social e da boa-fé, sempre presente a finalidade objetiva do contrato." (MARTINS-COSTA, 2000, p.403).

Como esclarece Paulo Nalin (1998, p. 195): "Não é dada à possibilidade de frustração das legítimas expectativas contratuais formuladas na esfera jurídica de qualquer dos contratantes devendo, ambos, proceder (conduta objetiva) comportamentalmente de boa-fé."

Mais uma vez é possível visualizar o papel da centralidade constitucional, considerando, sobretudo, que as ideias de boa-fé e função social são princípios gerais decorrentes da estrutura de direitos fundamentais estabelecida pela Constituição Federal.

Como afirma Paulo Luiz Lôbo Neto (2003, p. 206):

> A patrimonialização das relações civis, que persiste nos códigos, é incompatível com os valores fundados na dignidade da pessoa humana adotado pelas Constituições modernas inclusive pela brasileira (artigo 1º III). A repersonalização reencontra a trajetória da longa história da emancipação humana, no sentido de reposta a pessoa humana como centro do direito civil, passando o patrimônio ao papel de coadjuvante, nem sempre necessário[41].

Assim, o que se pretende definir é a visão de boa-fé "como regra de conduta fundada na honestidade, na retidão, na lealdade e, principalmente, na consideração para com os interesses do 'alter', visto como um membro do conjunto social que é juridicamente tutelado." (MARTINS-COSTA, 2000, p.403).

Deste modo, o grande desafio dos civilistas, para Paulo Luiz Lôbo Neto (2003, p. 206), passa a ser a visualização das pessoas em toda a sua dimensão ontológica e, através dela, o seu patrimônio, sendo essencial a materialização dos sujeitos de direito, que são mais que apenas titulares de bens, restaurando-se a primazia da pessoa humana nas relações civis.

Outra perspectiva interessante para o tratamento do presente tema é a compreensão do abuso de direito, a partir do princípio da boa fé objetiva como baliza para a averiguação da licitude no modo de exercício de direitos, vedando, por exemplo, o comportamento contraditório ou desleal, que, no presente tema, pode ocorrer quando o provedor que produz determinado Termo de Política de Privacidade descumpre as suas previsões.

Para Paulo Luiz Lôbo Neto (2003, p. 215), o juridicamente importante deixa de ser "a exigência cega de cumprimento do contrato, da forma como foi assinado ou celebrado, mas se

[41] Neste ponto deve ser referido o viés eminentemente "econômico" da interpretação dos institutos jurídicos, como trabalhado por Rodotá (2008).

a sua execução não acarreta vantagem excessiva para uma das partes ou desvantagem excessiva para a outra, aferível objetivamente pelos critérios de experiência ordinária."

O abuso de direito pode ser compreendido a partir do artigo 187 do Código Civil Brasileiro, como afirma Judith Martins Costa (2014, p. 34):

> Com efeito, para além de sustentar o que se poderia denominar de "casos tradicionais de abuso" – inclusive os decorrentes de desequilíbrio de posições jurídicas, em que o princípio (implícito) do equilíbrio conecta-se tanto ao princípio da boa-fé quanto à noção de fim econômico ou social do direito – a boa-fé do artigo 187 enseja, por conta de sua vocação sistematizadora, um virtuoso leque de possibilidades ao Direito brasileiro[42].

Assim, a visão de boa-fé objetiva é essencial para a compreensão do que é um comportamento ético, probo e honesto, o que se espera no tratamento dos dados pessoais fornecidos pelos usuários aos provedores de acesso à *Internet*. E este tratamento como decorrência do dever de informação tem que estar claro, preciso e disponível através dos Termos de Política de Privacidade.

Desta forma, estes termos podem ser juridicamente exigidos, pois apesar de não decorrerem expressamente da declaração de vontade, objeto principal do contrato de prestação de serviços entre usuário e provedor, decorrem dos deveres de informação que se originam da boa-fé objetiva.

Como esclarece Paulo Luiz Lôbo Neto (2003, p. 215), a boa-fé equidade entre as prestações constitui-se em um macro princípio da justiça contratual "que por sua vez abrange a boa-fé objetiva, a revisão contratual, o princípio do *venire contra factum proprio*, o princípio que veda a lesão nos contratos, a cláusula *rebus sic standibus*, a invalidade das cláusulas abusivas, a regra da *interpretatio contra stipulatorem*."

Assim, estes documentos – Termos ou Políticas de Privacidade – têm um papel primordial na garantia dos deveres de informação entre as partes, pois expressam a forma como os provedores pretendem proteger um importante direito fundamental dos seus usuários, a proteção à sua privacidade e dos seus dados pessoais.

[42] De acordo com Martins-Costa (2014, p. 36) "o princípio da boa-fé, por seu significado primacial de correção e lealdade, por sua inscrição em uma tradição sistematizadora, pela relativa vagueza semântica que o caracteriza – permitindo, em seu entorno, uma área de franja hábil a captar novas hipóteses não ainda tipificadas legal ou socialmente – mostra-se um instrumento da maior utilidade para resolver o "dilema do abuso", a saber: o de demarcar, no caso concreto, a extensão dos direitos e faculdades que não foram objeto de maior precisão legislativa."

2.2 A PROTEÇÃO DE DADOS NOS ORDENAMENTOS JURÍDICOS ARGENTINO, URUGUAIO E BRASILEIRO.

Compreendido que a proteção de dados pessoais é uma preocupação que perpassa os mais diversos graus de regulamentação, seja no nível internacional, regional e/ou comunitário, é essencial, para os objetivos deste trabalho, verificar e posteriormente comparar como as legislações nacionais dos países do Mercosul – com um nível adequado de proteção reconhecido pela União Europeia – regulamentam a matéria.

A legislação Argentina, pioneira no tratamento do tema nos países pertencentes ao Mercosul, regulamentou a proteção de dados pessoais ainda no ano 2000 com a Lei nº 25.326. Esta legislação adotou em grande parte aquilo que a União Européia, com a Directiva 95/46/CE, previa sobre a questão.

Esta lei dispôs claramente sobre as definições de dado pessoal e seu tratamento no Artigo 2º, vinculando sua utilização à finalidade para a qual eles foram captados – nos Artigos 4º e 11, além de regulamentar um procedimento de acesso e retificação quando necessário – Artigos 16 e 33 a 43, e criar um órgão específico de controle dentre outras previsões – no Artigo 29.

Oito anos depois, em 2008, a República Oriental do Uruguai, por meio da Lei nº 13.331, também passou a regulamentar especificamente a matéria, tratando de questões igualmente relevantes, porém de forma mais específica e direta que a legislação argentina, mas também fortemente influenciada pelas previsões da Directiva 95/46/CE.

Consta dentre as previsões da lei uruguaia, a definição de destinatário e processador de dados – no Artigo 4º, a responsabilidade no caso de violação da legislação – no Artigo 12, referindo expressamente a exigência de segurança de dados – no Artigo 10, além de, de forma semelhante à legislação argentina, regulamentar uma ação específica para fins de acesso e retificação de dados pessoais – nos Artigos 37 a 45 e, por fim, criando um órgão de controle independente na forma de uma Agência de Regulação de Controle de dados Pessoais (AGESIC) – nos artigos 31 a 35.

A Lei Argentina nº 25.326 de 2000 recebeu, em 30 de junho de 2003, através do Parecer nº 4/2002 do Grupo de Proteção de dados Pessoais da Comissão Européia, o título de país que assegura um nível adequado de proteção de dados pessoais (UNIÃO EUROPEIA, 2014-e).

Da mesma forma, a Lei Uruguaia nº 13.331 de 2008 recebeu em 21 de agosto de 2012, através do Parecer nº 6/2010 do Grupo de Proteção de dados Pessoais da Comissão Européia

(UNIÃO EUROPEIA, 2014-f), o título de país que assegura um nível adequado de proteção de dados pessoais.

Ao contrário dos outros países analisados, o Brasil ainda não disciplinou especificamente a matéria da proteção de dados pessoais. Na realidade a própria utilização da *Internet* apenas recentemente foi objeto de previsão legal, com a Lei nº 12.965 de 23 de Abril de 2014, mais conhecida como Marco Civil da Internet (BRASIL, 2014-a).

A Lei 12.965 de 23 de Abril de 2014 (Marco Civil da *Internet*) traz algumas previsões referentes à proteção de dados pessoais, mas que não trata especificamente desta matéria, que era objeto do projeto de Lei nº 4.060 de 2012[43] que pretendia normatizá-la[44] (BRASIL, 2014-b).

Deste modo haverá a análise das previsões do Marco Civil que tratam da proteção de dados pessoais em conjunto, quando necessário, com as previsões do projeto de futura lei brasileira de proteção de dados pessoais na *Internet*.

Com a finalidade de realizar uma comparação que se sustente cientificamente, foram eleitas determinadas categorias conceituais que serviram de critérios para esta análise, e que também justificaram a sua relação com a temática da segmentação comportamental, tema central do primeiro capítulo. Partindo desse critério, foram escolhidas/delimitadas as seguintes categorias: a) conceituação de dados pessoais e sua classificação/suas espécies; b) regulamentação do uso do dado sensível; c) consentimento do usuário para captação e uso dos dados de acordo com a finalidade prevista; d) veracidade dos dados pessoais registrados; e) procedimentos para acesso e retificação de dados; f) órgão de controle.

Com base nestas seis categorias, será feita a análise da condição destas legislações que foram consideradas com um adequado nível de proteção de dados pessoais pela União Européia, para proteger/tutelar os indivíduos, a partir do seu controle sobre os dados pessoais que lhes digam respeito – autodeterminação informativa.

2.2.1 A Lei nº 25.326/2000 e a proteção de dados pessoais na Argentina.

Inicialmente é preciso ressaltar que a legislação argentina parte de determinadas classificações de dados pessoais para dimensionar o seu grau de proteção, portanto é essencial

[43] Atualmente tal projeto de lei foi arquivado em 31 de Janeiro de 2015, conforme informação constante no site da Câmara Federal. (CÂMARA DOS DEPUTADOS, 2015).

[44] O Ministério da Justiça abriu em 28 de janeiro de 2015, consulta pública para a elaboração de um anteprojeto de lei sobre a "Proteção de Dados Pessoais", cujo consultor jurídico será Danilo Doneda. (BLOG DO PLANALTO, 2015)

compreender como o sistema argentino de proteção trata os dados pessoais, conforme a sua classificação.

A legislação argentina utiliza-se de diversos conceitos essenciais para a compreensão da forma de proteção que pretende garantir. Dentre eles, tem-se a conceituação do artigo 2º (ARGENTINA, 2014), onde dado pessoal é definido como "Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables[45]."

Conforme Pablo Palazzi (2004, p.11), "El eje de la protección de datos pasa por proteger la información personal. Si no hay datos personales o si estos están 'disociados'o 'anonimizados' o se trata de datos estatísticos 'impersonales' no cabe recurrir a la proteccíon de la ley[46]."

Algumas legislações, dentre as quais a argentina, "incluyen expresamente en la definición de datos personales no sólo a los registrados en documentos escritos o soportes informáticos, sino también a los constituidos por imágenes y sonidos[47]" (CARBÒ, 2001, p. 65).

Dado sensível, conforme o mesmo dispositivo significa "Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual [48]." (ARGENTINA, 2014).

Horácio Fernández Delpech (2004, p. 294) afirma que

> Para la ley argentina son unicamente datos sensibles los que revelan origen racial y étnico, opiniones politicas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud e a la vida sexual. El texto de la ley nos indica que se trata de una enumeración taxativa de los datos que se consideran sensibles. No se trata de una enumeración meramente enunciativa[49].

[45] Tradução do pesquisador: "qualquer informação, determinada ou determinavel relativa a pessoas físicas ou de existência ideal"

[46]Tradução do pesquisador: "o eixo de proteção de dados passa pela proteção da informação pessoal. Se não há dado pessoal ou se estes dados estão dissociados ou são considerados anônimos, ou se tratam de estatísticas impessoais, não cabe invocar a proteção da lei para isto."

[47]Tradução do pesquisador: "incluem expressamente na definição de dados pessoais não só os registrados em documentos escritos ou suportes informáticos, senão também os constituídos por imagens e sons."

[48] Tradução do pesquisador: "dados pessoais que revelem a origem racial ou étnica, opiniões políticas, crenças religiosas, filosóficas ou morais, a filiação sindical e dados relativos à saúde ou vida sexual."

[49]Tradução do pesquisador: "Para a lei argentina, são unicamente dados sensíveis os que revelam origem racial e étnica, opiniões políticas, convenções religiosas, filosóficas ou morais, afiliação sindical e informações referentes à saúde e à vida sexual. O texto da lei indica que se trata de uma enumeração taxativa dos dados que se consideram sensíveis. Não se trata de uma enumeração enunciativa, e esta característica da lei não permite incluir outros que não sejam especificamente mencionados."

Por outro lado, para Pablo Palazzi (2004, p. 16), esta previsão não deve ser considerada taxativa, pois não é necessário que determinado dado seja diretamente sensível, sendo que basta que potencialmente, por meio dele, seja possivel que se revelem informações desta mesma categoria, para que passe a ser considerado um dado sensível.

Nesta questão Pablo Palazzi (2004) aparentemente tem razão, pois na realidade o critério por excelência é a potencialidade de ocasionar discriminação que determinado dado possa gerar ao seu titular. Neste caso, ele deve ser considerado sensível e deve receber a proteção concedida pela legislação.

A legislação argentina especifica melhor as qualificações que esse dado deve ter em seu artigo 4º (ARGENTINA, 2014):

> 1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. 2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. 4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. 5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley. 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados[50].

Assim, os dados pessoais captados devem ter as seguintes características: devem corresponder à realidade, serem adequados, pertinentes e não excessivos em relação ao âmbito e propósito para o qual foram adquiridos. Esta previsão revela-se extremamente salutar, pois homenageia diversos princípios de proteção de dados pessoais surgidos na Diretiva 95/64 da União Européia, como a veracidade, a pertinência, e a finalidade.

Na realidade, a exigência de qualidade dos dados será "relevante en la medida en que la desatención de ese aspecto pueda generar perjuicios a los titulares de los datos. Si se trata

[50] Tradução do Pesquisador: "1 Os dados pessoais recolhidos para fins de tratamento devem ser verdadeiros, adequados, pertinentes e não excessivos em relação ao âmbito e propósito para o qual foram recolhidos. 2 A coleta de dados não pode ser feita por meio injusto, fraudulento ou contrário às disposições desta lei. 3 Os dados processados não podem ser utilizados para fins diferentes ou incompatível com as finalidades para as quais foram obtidos. 4 Os dados devem ser precisos e atualizados, se tal for necessário. 5. Informações total ou parcialmente imprecisas ou incompletas devem ser imediatamente removidas e substituídas pelo responsável pelo arquivo ou banco de dados quando este receber o conhecimento da imprecisão ou imperfeição das informações que precisa o caso, sem prejuízo dos direitos do titular referidos no artigo 16 desta lei. 6 Os dados devem ser armazenados de forma a permitir o exercício do direito de acesso do proprietário. 7 Os dados devem ser destruídos quando não forem mais necessários ou relevantes para os fins para os quais foram recolhidos.

de una base de datos para la publicidad, en principio, el error o vetustes de los datos no sólo perjudicará el interés o lucro de quien pretenda valer-se de ellos para tal fin[51]" (CARBÒ, 2001, p. 73), por exemplo, imputando uma oferta não desejada a um determinado indivíduo.

Outra questão importante constante no segundo item refere-se ao impedimento de captação de dados pessoais por meio fraudulento, injusto ou contrário à legislação. Esta previsão impede que um dado pessoal obtido de forma a ludibriar o titular venha a ser recolhido em um banco e após passe a identificar esta pessoa. Portanto, um eventual falso recadastramento para determinado serviço não pode servir como forma de obtenção de uma gama de informações de indivíduos para direcioná-los uma posterior publicidade.

Pablo Palazzi (2004, p. 31) cita como exemplos destes meios ilícitos:

> El robo de infomación o la obtención bajo falsas excusas, por ejemplo, la recopilación de datos en formularios para un sorteo que nunca se realizará, o la recopilación de datos en Internet, utilizando las fallas de seguridad en los sistemas informáticos, o su recogida mediante programa 'bots' o 'spiders' que recorren la red o la forma manual [...] La adquición pro medios desleales tiene lugar en la situación tan comun de soborno a empleados infieles que venden la información a terceros ajenos a la empresa[52].

O terceiro item deste dispositivo contempla de forma objetiva o princípio da finalidade no tratamento de dados pessoais como forma de deixar claro que a finalidade, informada no momento da captação, macula e vincula toda e qualquer utilização posterior deste dado pessoal.

Osvaldo Alfredo Gozaíni (2011, p. 196) afirma que: "En efecto, ningún archivo puede colectar datos que no estén vinculados con el fin que persigue su objeto, y de serlo surge um nuevo impedimiento para la interconexión en la medida que está prohibido desviar la información de su propósito original[53]."

O quarto item traz uma facultatividade preocupante, pois afirma que a atualidade e precisão dos dados ocorrerão quando necessário, porém esta previsão mantém a dúvida de quais são os critérios objetivos para se averiguar esta necessidade, e qual a autoridade

---

[51] Tradução do pesquisador: "relevante na medida em que a desatenção de um aspecto pode gerar prejuízo ao titular dos dados. Por exemplo, se for uma base de dados para publicidade, o erro ou desatualização dos dados não prejudicará somente o interesse de quem pretenda utilizá-los para tal fim".

[52]Tradução do pesquisador: "O roubo de informações ou a obtenção através de falsas expectativas, por exemplo, a recopilação de dados para um sorteio que nunca se realizará, ou a recopilação utilizando-se das falhas dos sistemas de segurança, mediante programas *bots* ou *spiders* que recorrem à rede ou de forma manual. [...] Ou como exemplo de meios desleais, tem-se o suborno de empregados que vendem informações a terceiros para prejudicar a sua empresa."

[53]Tradução do pesquisador: "Em efeito, nenhum arquivo pode coletar dados que não estejam vinculados com o fim que persegue seu objeto, e ao fazê-lo surge um novo impedimento para a interconexão na medida em que está proibido desviar a informação de seu propósito original."

responsável por esta verificação. Tal previsão deveria ser mais precisa, de forma a contemplar essas lacunas.

Por sua vez, o quinto item vincula os detentores de dados pessoais a manter a integridade de tais informações, também como forma de garantir que os atributos necessários ao dado a ser captado também sejam respeitados.

Portanto, o questionamento anterior está respondido pela previsão de que os responsáveis pelos bancos serão as entidades que devem corrigir eventual falha. Porém o dispositivo permanece com lacunas, pois não prevê consequências para os casos em que a correção não é feita.

Quanto ao entrecruzamento de dados, é possível afirmar que

> Ésta es una etapa técnica que produce la interrelación entre bancos de datos para lograr un perfil mejorado de la información que ellos contienen [...] Las condiciones y principios aplicables al archivo original son trasladados al que efectua el tratamiento, con particular atención en el deber de secreto y confidencialidad[54]. (GONZAÌNI, 2011, p. 272)

Por fim, o sexto e sétimo itens surgem como decorrência do direito do titular ao acesso e ao dever de respeito à finalidade da captação quando da utilização de dados pessoais, previsões que vêm a reforçar a aplicação dos princípios que a legislação elege como reitores do tratamento lícito de dados pessoais.

Outra questão relevante refere-se ao consentimento do titular do dado pessoal, tratada pela legislação argentina em seu artigo 5º (ARGENTINA, 2014):

> 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y

[54]Tradução do pesquisador: "Trata-se de uma etapa técnica que produz uma inter-relação entre os bancos de dados para obter um perfil melhorado da informação que eles já contem. [...] as condições e princípios aplicáveis ao arquivo original são transmitidos aos arquivos resultantes do tratamento, com especial atenção ao dever de segredo."

> de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526[55].

Este dispositivo prevê a regra da necessidade de consentimento livre, expresso e informado que deve ser conferido pelo titular para que determinado dado pessoal sobre sua personalidade seja tratado. Este consentimento torna-se essencial para que exista um efetivo respeito aos princípios comentados, sobretudo ao da finalidade, pois sem um consentimento não há como saber se esta informação será utilizada para a finalidade para a qual foi captada e se determinada utilização é apropriada a esta finalidade.

Assim "la ley requiere un consentimiento expreso, el que deberá constar por escrito (o por medios similares). Este consentimiento no puede ser inferido ni por el mero transcurso del tiempo ni por el silencio del titular de los datos[56]."(PALAZZI, 2004, p. 41-42)

A legislação argentina acertadamente exigiu que o consentimento fosse autorizado de forma explícita e em circulação, ou seja, além de ser obrigatório, deve manter-se integrado àquele determinado dado para evitar a sua utilização indevida.

O item seguinte refere-se às exceções à regra da exigência de consentimento, dentre as quais se tem três exceções lógicas: uma prevista na alínea "a", que decorre do local onde determinado dado foi captado – no caso em uma fonte de acesso público; e outras previstas nas alíneas "d" e "e", que decorrem da autonomia privada, como no caso do dado fornecido em decorrência de uma relação contratual em favor de determinada instituição financeira.

Preocupante a exceção prevista na alínea "b", ou seja, que abre uma brecha excessivamente ampla à atuação dos poderes públicos na captação de dados pessoais dos seus cidadãos. Para contornar esse problema, seria interessante se a legislação tivesse delimitado de forma mais precisa esta previsão, uma vez que autoriza os órgãos públicos a acessar os dados pessoais sem o prévio consentimento do titular, mesmo fora das hipóteses legalmente autorizadas.

---

[55] Tradução do pesquisador: "1 O tratamento de dados pessoais é ilegal quando o titular não tenha dado o seu consentimento livre, expresso e informado, que deverá ser por escrito ou por outros meios que serão equacionados de acordo com as circunstâncias. O referido consentimento dado com outras declarações devem aparecer de forma explícita e em circulação, mediante referência nos dados das informações descritas no artigo 6 desta lei. 2. O consentimento não é necessário quando: a) Os dados forem obtidos a partir de fontes de acesso público sem restrições; b) Recolhidos para o exercício de suas funções próprias dos poderes do Estado ou em virtude de obrigações legais; c) No caso de itens em que os dados são limitados a nome, identidade nacional, da segurança social ou de identificação fiscal, ocupação, data de nascimento e endereço; d) decorrentes de uma relação contratual, proprietário dos dados científico ou profissional, e são necessários para o seu desenvolvimento e implementação; e) É o caso de operações realizadas por instituições financeiras e as informações que recebem de seus clientes de acordo com as disposições do artigo 39 da Lei 21.526."

[56]Tradução do pesquisador: "a lei exige um consentimento expresso, que deve constar por escrito ou por meios similares. Este consentimento não pode ser inferido pelo transcurso do tempo nem pelo silêncio do titular dos dados."

Esta lacuna poderia possibilitar o avanço daquilo que alguns autores identificam como um Estado Vigilante (RODOTÀ, 2008), na medida em que os órgãos sempre alegam agir no exercício de suas funções, pois, do contrário, a sua atuação será em princípio ilícita, portanto o critério estabelecido na exceção seria demasiadamente generalista.

A previsão seria melhor delimitada se a legislação tivesse estabelecido que, no caso de interesse público devidamente justificado e que evidentemente impeça o exercício do consentimento livre e informado do titular dos dados, poderia haver o seu recolhimento.

Mais um ponto que merece referência é a questão da informação prévia que deve ser fornecida quando da captação do dado pessoal, contemplada no artigo 6º (ARGENTINA, 2014):

> Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos[57].

Tal dispositivo pretende, em primeiro lugar, possibilitar que o consentimento conferido pelo titular do dado pessoal efetivamente seja informado, isto é, que ele tenha as noções pertinentes e necessárias para consentir com a captação.

Alejandra M. Gils Carbó (2001, p. 81) afirma que a exigência de consentimento imposta pela lei "tiene su contrapartida en el derecho de oposición está implícito en la mención del art. 6 inc d) cuando dispones que la persona requerida debe ser informada sobre las consecuencias de proporcionar los datos y de la negativa a hacerlo[58]."

Dentre os elementos que devem constar desta informação, é essencial expressar a finalidade para qual serão tratados os dados pessoais, o que remete à previsão da vinculação

[57] Tradução do pesquisador: "Quando são recolhidos dados pessoais, devem ser previamente informados de forma explícita e clara: a) A finalidade para a qual serão tratados e quem podem ser os destinatários ou categorias de destinatários; b) A existência do arquivo, registro, banco de dados, eletrônico ou não, em questão, a identidade e o endereço do responsável; c) O carácter obrigatório ou facultativo das respostas ao questionário que é proposto, especialmente no que diz respeito aos dados reportados no artigo seguinte; d) As consequências de fornecer a informação, a recusa em fazê-lo ou inexatidão dos mesmos; e) A capacidade da pessoa em causa de exercer os direitos de acesso, retificação e supressão de dados."

[58] Tradução do pesquisador: "tem sua contrapartida no direito do titular de negar-se a fornecer seus dados pessoais, este direito de oposição está implícito no art. 6º d quando dispõe que a pessoa requerida deve ser informada sobre as consequências de fornecer os seus dados e da negativa de fazê-lo."

do tratamento destas informaçõesa esta finalidade, conforme já visto quando do comentário ao artigo 4º.

A legislação argentina ainda exige o detalhamento da destinação ao titular de direitos, devendo-se cientificá-lo se os dados obtidos serão direcionados a algum banco de dados, arquivo ou registro, e quem será o seu detentor.

Esta previsão é uma forma de possibilitar que haja um efetivo controle da finalidade da utilização do dado pessoal, além de evitar eventual segmentação ilícita dos dados, pois somente tendo informações suficientes sobre o tratamento é que haverá um adequado exercício de autodeterminação informativa, tema tratado por Pérez Luño (2005), um dos marcos teóricos dessa dissertação.

As informações referentes à obrigatoriedade das respostas que obtiveram os dados, bem como da existência de consequências para o internauta que deixa de fornecê-los, são importantes para a verificação e comprovação de que a captação foi feita de forma lícita.

Pelas previsões da lei argentina, o internauta deve ter a possibilidade de acessar, retificar ou suprimir determinadas informações. Essa garantia não só contribui para o exercício da autodeterminação informativa (PÈREZ LUÑO, 2005), como também é uma forma de vincular aquele que capta estes dados a garantir a efetividade dessas prerrogativas.

Outro ponto de destaque da legislação argentina é a preocupação com os dados sensíveis, pois na forma das previsões do artigo 7º (ARGENTINA, 2014):

> 1. Ninguna persona puede ser obligada a proporcionar datos sensibles. 2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros. 4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas[59].

[59] Tradução do pesquisador: "1 Ninguém pode ser obrigado a fornecer dados sensíveis. 2 Os dados sensíveis só podem ser recolhidos e tratados por razões imperiosas de interesse geral, autorizado por lei. Eles também podem ser tratados com fins estatísticos ou científicos quando os seus titulares não puderem ser identificados. 3. Bancos ou registros que armazenam informações que revelem direta ou indiretamente dados sensíveis são proibidos. No entanto, a Igreja Católica, associações religiosas e organizações políticas e sindicatos podem manter um registro de seus usuários. 4 Dados de contravenções ou histórico criminal só podem ser processados pelas autoridades públicas competentes, nos termos das respectivas leis e regulamentos."

Palazzi (2004, p. 63) afirma que “la definición de datos sensibles de la ley es clara: quedan incluídos dentro de este concepto todos los datos que de alguna manera puedan causar discriminación[60].”

Quanto ao uso do dado sensível, a legislação optou por exigir sempre que esta utilização ocorra somente da imperiosa necessidade decorrente de interesse geral, e autorizada por lei, permitindo-se o seu recolhimento com a finalidade estatística ou científica quando não houver identificação dos seus titulares.

Tais conceitos apresentam imprecisão, pois não há uma definição clara do significado da expressão “interesse geral”. Para tentar elucidar essa questão, Aljandra M. Gils Carbó (2001, p. 89) explica:

> En situaciones excepcionales en las que prevalezca el interés general sobre el particular de los individuos, ya sea por necessidade de la salud pública, defensa nacional, seguridad pública o social, para la protección de un interéss vital de lo interessado, etc. se permite el tratamiento del dato sensible [...] El procedimiento deliberativo que esta supone garantizaría, en la intención del legislador, el respeto a los derechos de los ciudadanos[61].

É possivel compreeender que

> no estamos aquí frente al caso del dato sensible voluntariamente aportado, sino de aquel que se considera útil e imprescindível para resolver un fin o destino que favorece al interéss general. Esté interés se colige de la ley no de la interpretación del titular o responsable del archivo, registro, base o banco de datos[62]. (GONZAÌNI, 2011, p. 257)

A própria legislação refere como exemplos de dados sensíveis aqueles relativos à saúde, a antecedentes criminais. A análise dessas previsões permite afirmar que a proteção neste ponto foi aquém da necessária, já que há informações como as educacionais e as familiares que deveriam ter o seu tratamento melhor delimitado, pois efetivamente configuram restrições a direitos fundamentais.

---

[60]Tradução do pesquisador: “a definição de dado sensível na lei é clara, e inclui dentro deste conceito todos os dados que de alguma forma podem causar discriminação, basta que com este potencialmente seja possível que esta discriminação ocorra”

[61]Tradução do pesquisador: “Em situações excepcionais onde prevaleça o interesse geral sobre o interesse particular, seja por razões de saúde pública, defesa nacional, segurança púlica ou social, para a proteção de um interesse vital do próprio interessado, etc., torna-se possível o tratamento de um dado sensível [...] O procedimento deliberativo que se supõe garantiria, na intenção do legislador, o respeito aos direitos dos cidadãos.”

[62]Tradução do pesquisador: “não estamos aqui frente ao caso do dado sensível voluntariamente recolhido, senão perante àquele que se considera imprescindível para resolver um fin ou destino que favorece a um interesse geral. Este interesse decorre da lei e não da interpretação do titular ou responsável pelo arquivo, registro, base ou banco de dados.”

O exame detalhado da legislação conduz a uma série de dúvidas decorrentes da excessiva abertura da redação dos dispositivos legais, carecendo de melhor explicitação sobre os limites que devem ser obedecidos pela legislação que excepcionar a regra da impossibilidade de captação de dados sensíveis, não definindo se estes limites constaram da Constituição Argentina, dos princípios e das normas internacionais de proteção de dados pessoais, etc.

Outra vedação que a legislação argentina apresenta é a manutenção de bancos de dados que possam revelar direta ou indiretamente informações sensíveis, e aqui também prevê uma exceção pouco delimitada que não está tratada especificamente no regulamento.

A exceção refere-se a determinados detentores de dados pessoais que poderiam manter bancos de dados sensíveis, autorização conferida de maneira ampla e que suscita alguns questionamentos, tais como: a) estas entidades somente podem manter dados pertinentes as suas finalidades? b) estas entidades não poderão trocar informações entre seus bancos de dados sensíveis?

Estas perguntas não são claramente enfrentadas no texto legal, o que indica que esta legislação poderia ter delimitado melhor esta exceção à vedação da manutenção de bancos de dados pessoais sensíveis.

Conforme explicitado por Horácio Férnandez Delpech (2004), infere-se da interpretação em conjunto dos artigos 5º e 7º da legislação que, mesmo que haja a concordância do titular dos dados sensíveis, sua captação não pode ocorrer em determinados casos previstos nas exceções do artigo 7º, norma particular que excepciona a regra geral do artigo 5º.

As previsões até então referidas e comentadas têm por finalidade garantir ao titular dos dados o exercício de um direito fundamental ao acesso aos seus registros, além das possibilidades de retificá-los e até mesmo suprimi-los se assim lhe convier.

Para que o titular possa efetivamente exigir o respeito e cumprimento dos princípios e regras até então estabelecidos, a legislação argentina lhe concede o acesso aos seus dados pessoais no Artigo 14 (ARGENTINA, 2014):

> 1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. 2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley. 3. El

> derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. 4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales[63].

Aqui se tem a previsão do direito ao acesso aos dados pessoais pelo titular, condicionando este acesso apenas à comprovação da sua própria identidade, não exigindo qualquer exposição de motivos ou razões para o exercício deste direito, o que demonstra que a regra geral será sempre o livre acesso aos dados disponibilizados.

Como esclarece Pablo Palazzi (2004, p. 111): "la ley no dice quién deve presentarse el pedido de acceso, pero se entende que debe serlo antes quien tenga a sua cargo el banco de datos. En cierta emplesa existe un empleado dedicado a tratar los temas de privacidad, que puede ser quien reciba tal pedido[64]."

O mesmo doutrinador (PALAZZI, 2008, p. 111) aponta um problema no fato de que a lei argentina:

> [...] lamentablemente, no contempla la posibilidad de prórroga de plazos para la entrega de la información. Esto tiene relevancia en el caso de pedidos masivos, donde el titular de la base de datos no puede responder a una grande cantidad de pedidos o cuando se necessita más tiempo para realizar una investigación interna a fin de encontrar la información[65].

A legislação fixa um prazo para a efetivação deste direito, após o qual será ajuizada uma ação específica para a obtenção dos dados pessoais e para a efetiva fruição do direito ao acesso.

Analisando esta previsão, percebe-se que, se por um lado a fixação de prazo exíguo pode ser salutar por permitir o efetivo acesso, por outro lado tal procedimento pode caracterizar-se como um entrave à futura eventual ação, pois a legislação aparentemente exige

---

[63] Tradução do pesquisador: "1 O proprietário dos dados, com a prova de sua identidade, tem o direito de solicitar e obter informações sobre os seus dados pessoais nas bases de dados públicas, ou privadas destinadas a relatórios. 2 O controlador ou usuário deve fornecer as informações solicitadas no prazo de dez dias corridos após ser intimado de forma confiável. Após esse período, se não satisfeita a ordem, ou se a satisfação for considerada insuficiente, será ajuizada a ação para a proteção de dados pessoais ou *habeasdata* previstos na presente lei. 3 O direito de acesso a que se refere o presente artigo só pode ser exercido sem qualquer custo em um prazo não inferior a seis meses, a menos que um interesse legítimo justifique que se desconsidere este intervalo. 4 O direito a que se refere este artigo, no caso de dados relativos a pessoas mortas, será garantido aos seus sucessores universais."

[64] Tradução do pesquisador: "a lei não disse a quem se deve apresentar o pedido de acesso, porém se entende que deve ser quem tenha a seu cargo o banco de dados, em certas empresas existe um empregado dedicado a tratar os temas pertinentes à privacidade, que pode ser quem deve receber o pedido."

[65] Tradução do pesquisador: "[...] lamentavelmente não ter previsto a possibilidade de prorrogação do prazo para o fornecimento, o que pode prejudicar determinados detentores de bancos de dados que recebam pedidos em grande quantidade ou quando for necessário um tempo maior para que se realize uma investigação interna para a obtenção do dado solicitado."

que um procedimento anterior ocorra, o que poderia ficar prejudicado em face do reduzido prazo previsto.

O procedimento previsto por este dispositivo refere que o direito ao acesso ocorrerá após a intimação de forma confiável, porém este mesmo dispositivo não esclarece, de forma objetiva, qual o órgão deverá determinar, no caso concreto, se a intimação deve ser considerada confiável.

Esta lacuna poderia dificultar o direito ao acesso, visto que o reponsável pelo banco de dados pode alegar que a intimação não foi feita de forma confiável e negar ao titular o seu exercício.

A limitação temporal para o exercício gratuito do direito ao acesso pode configurar-se como um obstáculo a esta garantia, uma vez que, em conjuto com a previsão anteriormente referida, poderia ocorrer uma determinada situação onde o responsável pelo dado entenda que as intimações apresentadas não são confiáveis até o momento em que transcorra o período de seis meses, e o exercício deste direito deixe de ser gratuito.

A legislação prevê que tal prazo para o exercício gratuito poderia ser desconsiderado no caso de um legítimo interesse do titular, porém, da mesma forma como não regulamenta qual o ente deverá julgar se determinada intimação é confiável, deixa de prever a quem cabe este juízo de legitimidade.

Quanto à legitimidade dos sucessores, trata-se de uma previsão correta, considerando que mesmo as pessoas falecidas permanecem com alguns direitos tais como a honra, a imagem e o nome, e quem legitimamente deve defendê-los são os sucessores do titular.

Porém a mera previsão do direito ao acesso como contemplado no dispositivo anteriormente comentado não seria capaz de garantir por si só o seu exercício e, atentando-se a isto, a legislação argentina regulamentou a forma com que tal informação deve estar disponibilizada, conforme previsto no artigo 15 (ARGENTINA, 2014):

> 1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. 2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin[66].

[66] Tradução do pesquisador: “1 Devem ser fornecidas as informações de forma clara, livre de codificações e se for acompanhado de uma explicação em conhecimento leigo da população média dos termos utilizados. 2 A informação deve ser global e lidar com todo o registro pertencente ao proprietário, mesmo que o único requisito para compreender um aspecto de dados pessoais. Em qualquer caso, o relatório pode divulgar os dados

Tal dispositivo evita expressamente que o fornecimento das informações seja feito através de uma linguagem tão técnica e específica que o titular dos dados não as compreenda, o que tornaria o exercício do direito ao acesso evidentemente inócuo.

Como esclarece Palazzi (2004, p. 115):

> En la práctica, los bancos de datos utilizan codificaciones que les permiten ahorrar memoria informática, agilizar las búsquedas y a la vez intercambiar y entrecruzar datos em forma mas rápida y eficiente [...] Estos códigos se justifican desde un punto de vista técnico en el ahorro de memória, dado que miliones de datos hacen pelas bases de datos [...] Por eso la norma en comentário aclara que el acceso a estos datos debe tener lugar com una explicación del significado de los mismos[67].

Ainda, tal dispositivo evita que a informação seja fornecida de forma fragmentada, o que também tornaria a compreensão de tais dados mais complexa por aquele titular que pretende acessá-los. Este cuidado evita que, no próprio processo de acesso a dados pessoais, ocorra uma segmentação de informações, de forma a possibilitar que o titular acesse os seus dados, mas não tenha a compreensão da magnitude de informações arquivadas a seu respeito.

Estes cuidados com a condição em que os dados serão disponibilizados são necessários em face da excessiva vulnerabilidade técnica do consumidor[68], visto que caso não houvesse esta previsão expressa ele teria somente uma visão fragmentada de todas as informações que são extraídas dos seus dados. E, deste modo, o usuário consumidor, deveria ter conhecimentos técnicos para compreender a totalidade das informações, considerando a qualidade não integral de sua disponibilização.

O terceiro dispositivo refere-se propriamente à forma como a informação será prestada, na configuração como o titular solicitar, seja por escrito, através de um telefonema, por uma comunicação eletrônica, dentre outras modalidades. Tal amplitude é vantajosa das

---

pertencentes a terceiros, mesmo quando ligado a essa pessoa. 3 Informações por opção do titular podem ser prestadas por escrito, por telefone, imagem eletrônica ou outro meio adequado para este fim."

[67]Tradução do pesquisador: "Na prática, os bancos de dados utilizam codificações que lhes permite utilizar a memória informática, agilizar as buscas e cruzar dados de forma mais rápida e eficiente. [...] Estes códigos se justificam do ponto de vista técnico para auxiliar a memória, visto que milhões de dados passam pelas bases de dados. [...] Por esta norma, quando do acesso a estes dados, deve ocorrer uma explicação do significado destes códigos"

[68] A *Constitucion De La Nacion Argentina* preleciona em seu Articulo 42 que: "Los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a una información adecuada y veraz; a la libertad de elección, y a condiciones de trato equitativo y digno" e esta previsão constitucional é regulamentada pela *Ley de Defensa Del Consumidor*, a Lei nº 24.240 de 1993, que contempla a idéia de vulnerabilidade técnica de forma semelhante a legislaçaõ brasileira, como será tratado mais a frente. (ARGENTINA, 2014-a)

formas, pois o titular não precisará aguardar o retorno de uma comunicação escrita para ter acesso aos dados arquivados a seu respeito.

Esta previsão tem um importante papel, pois tampouco o internauta precisará realizar deslocamento físico, o que dificultaria o acesso, pois poderá utilizar outros meios para poder ter acesso aos dados de forma rápida, com reduzido custo e maior eficiência. Porém há o problema da forma oral de solicitação é que ele ficará apenas com um protocolo ou com meios de prova por vezes discutíveis quando ao conteúdo da sua solicitação[69].

Outro ponto forte da lei refere-se à possibilidade de retificação, atualização ou supressão de dados pessoais, que decorrem naturalmente do direito ao acesso a tais informações, o que está previsto no artigo 16 da legislação argentina (ARGENTINA, 2014):

> 1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. 2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. 3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de corpus data prevista en la presente ley. 4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato. 5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos. 6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión. 7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos[70].

[69] No caso do Brasil com a possibilidade de inversão do ônus da prova, franqueada pelo art. 6º VII da Lei nº 8.078/1990 (Código de Proteção e Defesa do Consumidor) este problema poderia ter os seus efeitos minorados.

[70] Tradução do pesquisador: "1 Toda a pessoa tem o direito de que sejam retificados, atualizados e, se for o caso, suprimidos ou sujeitos a confidencialidade dos dados pessoais referentes a ela, que estão incluídos em um banco de dados. 2 O responsável ou usuário do banco de dados deve proceder retificação, exclusão ou atualização de dados pessoais, realizando as operações necessárias para fazê-lo em um prazo máximo de cinco dias úteis após a recepção do pedido do titular dos dados, ou do momento em que tomar conhecimento do erro ou falsidade. 3º descumprimento ao prazo constante no item anetrior autorizará o titular a ajuizar de imediato a ação de proteção de dados ou *habeas data* previstos na presente lei. 4 Em caso de cessão ou transferência de dados, a pessoa ou o usuário do banco de dados deve notificar a correção ou eliminação para o cessionário no prazo de cinco dias úteis após o tratamento dos dados feitos. 5 A exclusão não se aplica quando poderia causar danos aos legítimos direitos ou interesses de terceiros, ou quando há uma obrigação legal de retenção de dados. 6 Durante o processo de verificação e correção do erro ou falsidade da informação em questão, a pessoa ou o usuário do banco de dados deve ou bloquear o arquivo, ou consignar que forneça informações relativas ao fato de que ele está sujeito à revisão. 7 Os dados pessoais devem ser conservados durante o período especificado no contrato entre o responsável ou usuário do banco de dados e o proprietário dos dados."

Depois de garantido o acesso a dados pessoais que lhe digam respeito, o titular deverá também ter o direito a corrigir tais informações quando estejam equivocadas, atualizá-las, quando não correspondem mais a realidade, ou ainda, suprimi-las quando não deseja que a informação a seu respeito persista junto aos bancos de dados.

Verifica-se que a lei argentina evidencia seguir a tendência da legislação européia, mais precisamente da legislação espanhola[71] ao privilegiar o direito ao esquecimento, já antecipando um tema que apenas atualmetne tem sido motivo de preocupação no ordenamento jurídico brasileiro[72].

Esta previsão protege o denominado "direito ao esquecimento" que "corresponde ao *derecho al olvido* presente no direito espanhol, constituindo-se em um aspecto das prestações do direito a intimidade. [...] Portanto, os dados devem ser guardados por um tempo determinado, não podem ser utilizados eternamente." (LIMBERGUER, 2007, p. 199)

Para compreender este direito ao esquecimento é preciso considerar que o direito à privacidade e o direito à intimidade visam, de uma forma geral, garantir ao ser humano um círculo indevassável sobre o "hoje" e o "agora", cada qual com o seu respectivo raio, desta forma:

> O indivíduo deve ter a garantia de que não será importunado por elementos trazidos do passado. Nem sempre o indivíduo pretende participar, ou continuar participando, da vida como personagem principal do interesse alheio. Trata-se, pois, de um dever de abstenção em relação à pessoa, que deve ser preservada também nesse aspecto. Vale destacar que o objetivo dessa proteção é o esquecimento enquanto fato jurídico, ou seja, deve haver relevância para o universo do direito (RAMOS, 2014, p. 12).

Registre-se também que a lei contempla a possibilidade de imposição de confidencialidade a determinados dados pessoais. Essa previsão entrega a classificação destas informações pessoais ao seu titular, o que também pode ser caracterizado como um efetivo exercício de autodeterminação informativa (PÈREZ LUÑO, 2005).

A possibilidade de atribuição de confidencialidade é importante na medida em que determinado titular pode não se opor a permanência de algumas informações a seu respeito em um arquivo, porém tenha a intenção de que tal dado não fique disponibilizado a um número indeterminado de entes.

---

[71] Tal direito encontra previsão no art. 27.2 da LO 5/92 da Espanha. (LIMBERGUER, 2007, p. 54).

[72] Atualmente o ordenamento jurídico brasileiro passou a tratar do "direito ao esquecimento" no Enunciado nº 531 da IV Jornada de Direito Civil que previu "A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento." (JUSTIÇA FEDERAL, 2014)

A imposição de um prazo para responsável pelo banco de dados proceder à retificação, atualização, supressão ou atribuição de confidencialidade sobre determinado dado é uma medida salutar para a proteção dos indivíduos titulares, pois de nada adiantaria garantir o direito a esta solicitação se não houvesse um prazo para o seu cumprimento, conforme o segundo item.

Na forma estabelecida no terceiro item, o descumprimento do pedido ou o seu cumprimento fora do prazo de cinco dias possibilita ao titular o ajuizamento da competente ação de proteção de dados pessoais, e ou *habeas data* na forma desta mesma legislação argentina[73].

A exclusão de dados pessoais não ocorrerá quando houver a possibilidade de ocasionar danos a terceiros, ou quando houver alguma obrigação legal de retenção de dados. Quanto a esta previsão, obviamente tal limitador é uma decorrência da autodeterminação informativa, visto que estes terceiros também têm o direito de ser informados sobre a possível exclusão dos seus dados.

Nesta situação há uma colisão de direitos fundamentais pertencentes a diferentes indivíduos, pois a supressão de um determinado dado pessoal de um indíviduo, apesar de privilegiar a sua autodeterminação, pode ocasionar a exclusão de informações pessoais titularizadas por outros, cujas informações estão vinculadas àquelas, realizando um tratamento de dados pessoais sem o consentimento deste segundo titular.

Para solucionar o referido conflito deve-se recorrer, a partir de parâmentros objetivamente estabelecidos, a ponderação de bens e valores[74] para que seja possivel constar se em determinado caso concreto o direito daquele que pretende suprimir os seus dados deve ou não prevalecer sobre os direitos daqueles titulares dos dados vinculados.

Por fim, tem-se a previsão de que os dados devem ser conservados pelo período acordado em contrato entre o titular desses direitos e o detentor do banco de dados, o que evita que, mesmo após o fim de determinada contratação, a empresa persista com os dados pessoais de diversos titulares, e coibe que ele pratique a segmentação comportamental ilícita.

Outra previsão pertinente para a temática da segmentação comportamental consta do artigo 27 (ARGENTINA, 2014), que trata dos arquivos, registros ou bancos de dados para a publicidade:

---

[73] Por outro lado, o quarto ítem estende aos cessionários que eventualmente recebam determinado dado pessoal a obrigação de cumprir os pedidos de retificação de dados pessoais que estejam sob sua guarda.

[74] Esta poderação deve ser feita apartir dos critérios da necessidade, da adequação e da proporcionalidade em sentido estrito (ALEXY, 2008), sempre considerando as peculiaridades do caso concreto, como já estudado no capitulo anterior.

> 1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. 2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. 3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo[75].

Assim, a legislação argentina trouxe a previsão de que a utilização de dados pessoais para fins publicitários é possível, desde que condicionadas a sua prévia disponibilização pública ou que o titular tenha concedido o seu livre, expresso e informado consentimento. Porém, mesmo nesta hipótese o titular não perde a sua autodeterminação informativa, visto que sempre deverá ter o direito ao acesso gratuito a tais dados, bem como sua posterior retificação, supressão ou atualização.

Como esclarece Rosane Leal da Silva (2010, p. 3914):

> No que tange aos dados recolhidos com a finalidade de posteriormente serem empregados para fins publicitários, algo bastante comum no Brasil, a lei argentina dispõe, no artigo 27, que na publicidade de venda direta e atividades análogas é permitido tratar dados que sejam aptos a estabelecer o perfil do consumidor, de forma que a partir deles se estabeleçam hábitos de consumo, desde que esses dados figurem em documentos acessíveis ao público ou tenham sido facilitados pelos próprios titulares, ou seja, que o titular voluntariamente tenha autorizado o acesso aos seus dados. Mesmo no caso de autorização expressa para a obtenção e uso dos dados, o titular poderá em qualquer tempo ter acesso ao que foi recolhido, bem como solicitar que as informações referentes a sua pessoa sejam retiradas daquele banco de dados.

Viasualiza-se, portanto, que a legislação argentina não optou por vedar o *Database Marketing*, somente limitou o seu exercício, o que para aquele país mostrou-se a melhor solução para aliar os interesses econômicos dos detentores de bancos de dados com os direitos fundamentais dos titulares.

Para o exercício dos direitos ao acesso e as consequentes possibilidade de retificação, supressão, atribuição de confidencialidade, dentre outros, a legislação argentina estabelece uma ação específica em seu artigo 34 (ARGENTINA, 2014): "La acción de protección de los

[75] Tradução do pesquisador: "1 Na coleção de domicílios, compartilhamento de documentos, publicidade ou vendas diretas e atividades similares, podem ser processados dados adequados para estabelecer determinados perfis com fins promocionais, comerciais ou de publicidade; ou para estabelecer hábitos, quando aparecem em documentos publicamente disponíveis ou foram fornecidas pelo titular com o seu consentimento. 2 Nos casos referidos no *caput* deste artigo, o titular dos dados pode exercer o direito de acesso, sem custos adicionais. 3 O titular poderá, a qualquer momento, solicitar a remoção ou o bloqueio do nome dos bancos de dados a que se refere este artigo."

datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado[76]"

Osvaldo Alfredo Gozaíni (2011, p. 401) afirma que a lei argentina

> habilita un procedimiento para la proteccion de los datos personales por el que se destaca la amplitude prevista para la legitimación activa. [...] El derecho a tutelar los datos no se visualiza como un derecho subjetivo, individual y personalísimo. Pareciera plantearse al dato como un problema de propriedade a defender[77].

O polo passivo desta demanda será composto pelos responsáveis e usuários de bancos de dados públicos e privados, conforme artigo 35 (ARGENTINA, 2014), sendo que a competência será concorrente entre o juízo do requerente, o domicílio do requerido, o lugar onde o ato ou fato ocorreu, e será de livre escolha do autor, conforme o artigo 36 (ARGENTINA, 2014).

A competência ser concorrente entre o domicilio do requerido e o lugar onde o ato ou fato ocorreu tem duas implicações importantes para a proteção do direito do cidadão titular dos dados pessoais:

Em primeiro lugar, pois ao ampliar o âmbito da competência para a ação a lei argentina facilita o seu exercício ao internauta, pois torna desnecessário o seu declocamento ao local sede do responsável pelo banco de dados.

E, em segundo lugar, auxiliar na aplicabilidade da própria legislação, pois muitas vezes os responsáveis pelo registro estão localizados em outros países não abrangidos pelas mesmas prerrogativas da lei de proteção de dados argentina, e podem utilizar-se disso para se eximir de cumprir suas previsões.

As previsões dos polos da ação – tanto ativo como passivo – bem como do juízo competente são extremamente salutares, pois estendem ao ente que se utiliza de bancos de dados o dever de garantir o direito ao acesso e os seus consectários ao titular destas informações.

Tal demanda deverá preencher os requisitos previstos no artigo 38:

---

[76]Tradução do pesquisador: "A ação para a proteção de dados pessoais ou *habeas data* pode ser exercida pelo afetado ou responsáveis e seus sucessores dos indivíduos, seja em linha retaou colateral até o segundo grau, por si ou através de procuração."

[77]Tradução do pesquisador: "habilita um procedimento para a proteção dos dados pessoais por meio do qual se destaca a amplitude prevista para a legitimação ativa [...] o direito a tutelar os dados não se visualiza como um direito subjetivo, individual e personalíssimo. Parecendo tornar-se o dado um problema de propriedade a defender."

> 1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen. 2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley. 3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial. 4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. 5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio[78].

Nota-se que, dentre os requisitos para a demanda de proteção de dados pessoais, não consta necessariamente a submissão aos procedimentos previstos nos artigos 14 e 16, o que demonstra ser possível ao internauta o ajuizamento direto e imediato da competente ação.

Além disto, as exigências de precisão narrativa, bem como de argumentação sucinta são salutares, pois possibilitam uma rápida tramitação da demanda, além de garantir que o acesso, e seus direitos consequentes, sejam exercidos com a maior breviedade possível.

A solicitação, por parte da vítima, que conste nos dados que as informações, objeto do seu pedido de retificação, estão sujeitas a um processo, funciona como uma forma eficaz de evitar que estas informações possam lhe ocasionar prejuízos durante a sua tramitação.

Outra previsão protetiva consiste na possibilidade de o juiz bloquear o acesso ao arquivo relacionado ao julgamento, se este puder ocasionar discriminação do titular destes dados.

Trata-se de uma medida preventiva que visa proteger o titular do dado pessoal durante o procedimento ajuizado e que se configura como a autorização para a concessão de uma

---

[78] Tradução do pesquisador: "1 A reclamação deve ser apresentada por escrito, identificando com a maior precisão possível, o nome e endereço do arquivo, registro ou banco de dados e, se for o caso, o nome da pessoa ou usuário da mesma. No caso de arquivos, registros ou bancos públicos, procurará estabelecer a agência estatal de que dependem. 2 O autor deve alegar as razões que entende que estejam gravadas ou reproduzidas no arquivo, as informações individualizadas em banco de dados a respeito de sua pessoa; as razões pelas quais considera que a informação relevante é discriminatória, falsa ou inexata e justificar que eles tenham cumprido as finalidades que fazem o exercício dos direitos nos termos desta lei. 3 A vítima pode solicitar que durante a duração do processo, no registro em banco de dados conste que aquelas informações estão submetidas a um processo. 4 O juiz pode ordenar o bloqueio provisório do arquivo em relação ao julgamento de dados pessoais quando se trate de informação discriminatória, falsa ou inexata evidente em questão. 5 A fim de solicitar informações do arquivo, registro ou banco de dados envolvidos, o critério legal para avaliar as circunstâncias exigidas nos pontos 1 e 2 deve ser abrangente."

tutela inibitória, que significa um avanço por romper com a dogmática tradicional de prevalência da tutela ressarcitória, baseado no binômio "lesão-reparação."

Como esclarece Ricardo Luiz Lorenzetti (1998, p. 337) para tratar de direitos fundamentais "desenvolveu-se a consciência de que é urgente conceber instrumentos de realização efetiva. A saúde, a intimidade, a identidade pessoal, as condições gerais dos contratos, são subjetivados e assistidos de um modo típico, através da tutela civil inibitória."

Na realidade a mera reparação ou resasarcimento pela violação a direitos fundamentais é uma resposta geralmente tardia que privilegia uma visão patrimonialista do direito privado em lugar de proteger a dignidade da pessoa humana do titular do direito violado. Portanto esta previsão da legislação argentina é salutar, pois autoriza o juízo a inibir preventivamente o acesso a dados pessoais que possam ser prejudiciais ao titular.

Como esclarece Ricardo Luiz Lorenzetti (1998, p. 337):

> Nos direitos fundamentais há um tempo próprios e distintos daquele previsto nas tradicionais formas de ação e da proteção substantiva; estão vinculados a situação existencial do indivíduo. A proteção ressarcitória colide com a situação contextual e, não a modificando, é distorcido o resultado definitivo do processo.

Após o ajuizamento da demanda, conforme artigo 41 (ARGENTINA, 2014), haverá a resposta ou defesa do detentor do banco de dados pessoais, que, por sua vez, deve indicar as razões pelas quais incluiu a informação questionada, ou ainda, porque não a retirou do arquivo conforme o pedido formulado pelo requerente, em conformidade com o disposto nos artigos 13 a 15.

É necessário identificar que o valor que esta legislação busca proteger é a privacidade dos individuos, como afirma Orlando Pulvirenti (2013, p. 51):

> En 2003, en la denominada causa 'spam', el juzgado interveniente dispuso por vía cautelar, sobre la base de la ley 25.326, que el afectado tenía derecho a acceder a sus datos y a solicitar ser removido de la base en la que se encontraba dicha información, por lo que podía evitar el correo no deseado[79].

Com base nesta resposta do responsável pelo banco de dados, o autor da demanda, titular do dado pessoal, poderá "ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que

[79]Tradução do pesquisador: "Em 2003, no denominado 'caso spam' o julgador interveniente dispôs, por via cautelar, com base na Lei 25.326, que a vítima teria direito de acessar os seus dados e solicitar que fossem removidos da base em que se encontravam determinadas informações, como forma de evitar o correio indesejado"

resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente[80]", conforme artigo 42 (ARGENTINA, 2014).

Por fim, quando do julgamento, o juízo decidirá na forma do artigo 43 (ARGENTINA, 2014):

> 1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia. 2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. 3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante. 4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto[81].

Assim o juiz decidirá se realmente as informações devem ser retificadas, removidas, atualizadas, ou, ainda, se a elas deve ser atribuída à confidencialidade, conforme a intenção do titular, o que não exclui a possibilidade de uma ação de responsabilidade civil para reparação de quaisquer outros danos que ele possa ter sofrido.

Verifica-se que há uma interface entre a via administrativa e a via judicial de exercício dos direitos concedidos pela legislação, se, por um lado, o órgão de controle pode ingressar em juízo para fazer valer as previsões da legislação em determinadas situações, por outro, quando da decisão final o juízo também deverá comunicar ao órgão, qualquer que seja o resultado do julgamento.

Por fim, a última previsão legal que merece uma referência é aquela que regulamenta a entidade governamental criada com a função específica de exigir o cumprimento destas normas, conforme prevê o artigo 29 (ARGENTINA, 2014):

> 1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza; b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las

[80]Tradução do pesquisador: "âmbito de aplicação, solicitando exclusão, retificação, confidencialidade ou atualização dos seus dados pessoais, nos casos decorrentes nos termos desta lei, oferecendo o mesmo ato as provas pertinentes."

[81] Tradução do pesquisador: "1 Expirado o prazo para resposta ou apresentada a contestação, ou ainda, no caso do artigo 42, após o alargamento, e tendo se produzido a prova, o juiz irá sentenciar. 2 Em sendo julgada procedente a ação, o juiz deverá especificar se as informações devem ser removidas, retificadas, atualizadas ou declaradas confidenciais, estabelecendo um prazo para o cumprimento. 3 No caso de julgamento improcedente da ação, esta não constitui caso *prima facie* de responsabilidade que podem ser efetuadas pela recorrente. 4 Em qualquer caso, a decisão deve ser comunicada ao órgão de controle, que deve registrar o seu efeito"

> actividades comprendidas por esta ley; c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley[82].

Tal órgão, como é possível visualizar, tem diversas atribuições, dentre as quais se destacam uma função de mediação da relação entre os titulares dos dados e os detentores dos arquivos, registros ou bancos que contenham tais dados, com o objetivo de garantir os direitos dos primeiros, sem inviabilizar as atividades dos segundos; uma função de fiscalização, sancionando os entes que descumprem as medidas previstas nesta legislação, tanto no âmbito administrativo como no âmbito penal, titularizando eventuais ações penais; o órgão também funciona como um instrumento de registro, realizando um recenseamento dos bancos de dados existentes e dos seus titulares e responsáveis, o que é uma atividade extremamente útil, pois subsidia os titulares no exercício do seu direito ao acesso e consectários.

Considerando as crises decorrentes da excessiva burocratização dos procedimentos e da situação de sobrecarga de processos enfrentada pelos órgãos do Poder Judiciário nos mais diversos países, a existência de um órgão administrativo surge como uma forma de efetivar as previsões da legislação.

---

[82] Tradução do pesquisador: "1 O órgão de fiscalização realizará todas as ações necessárias para cumprir os objetivos e outras disposições da presente lei. Para este efeito, terá as seguintes funções e competências: a) Ajudar e aconselhar as pessoas que necessitam dele no âmbito desta lei e os meios legais disponíveis para defender os direitos nela garantidos; b) Emitir normas e regulamentos a serem observados no desenvolvimento das atividades abrangidas pela lei; c) Realizar um recenseamento de arquivos, registros ou bancos de dados feitos pela lei e manter um registro permanente dos mesmos; d) Acompanhar o cumprimento das regras de segurança de dados, arquivos, registros ou bancos de dados. Para efeito, pode solicitar autorização judicial para entrar nas instalações, equipamentos ou programas de processamento de dados, a fim de verificar as violações em conformidade com este Estatuto Social; e) Solicitar informações a entidades públicas e privadas, que devem fornecer os registros, documentos, programas ou outros itens relativos ao tratamento de dados pessoais. Nesses casos, a autoridade deve garantir a segurança e confidencialidade dos elementos de informação fornecidos; f) Impor sanções administrativas aplicáveis no caso de violação desta lei e dos regulamentos a serem emitidas em sua consequência; g) Tornar-se autor da denúncia em ação penal por violações promovidas na formadessa Lei; h) Fiscalizar o cumprimento das exigências e garantias a serem cumpridas por arquivos privados ou bancos que fornecem dados para relatórios, para obter a entrada correspondente no registo estabelecido por essa lei. [...]"

Sobretudo, pois de nada adiantaria legislar sobre os dados pessoais sem ter uma estrutura compatível para assegurar o cumprimento da lei, o que deve ser feito na via administrativa num primeiro plano, especiamente considerando que o Poder Judiciário está sempre tão sobrecarregado.

Com isto, verifica-se que a legislação argentina apresenta um grau de proteção razoável, apesar de em muitos aspectos trazer previsões excessivamente generalistas, sobretudo quando trata de exceções a determinados princípios fundamentais, como o do consentimento ou da finalidade.

Essa legislação regulamenta a necessidade de consentimento para a captação do dado pessoal, distingue o tratamento de dados conforme a sua natureza – sensível e não sensível – ,além de prever o direito ao acesso, retificação, atualização e atribuição de confidencialidade, e os instrumentos para o seu exercício e, por fim, traz a previsão da criação de um órgão estatal de controle específico para tratar das questões pertinentes a referida lei.

2.2.2 Os dados pessoais na ordem jurídica do Uruguai: a Lei nº 18.331/2008.

Inicialmente é essencial referir que a legislação uruguaia está sustentada em uma gama de principios de proteção dos dados pessoais a partir dos quais o sistema foi construído, e opta por nomear expressamente estes princípios em seu art. 5º (URUGUAI, 2014), ao contrário da legislação argentina, onde a principiologia decorre das previsões legais.

Isso se deve à própria natureza eminentemente principiológica daquele sistema jurídico, como afirma Hector Delpiano (2003, p. 415):

> Uruguay cuenta con un coherente sistema de protección de los derechos fundamentales sustentado en una estructura jurídica cuyo principal pilar está dado por un grupo normativo constituido por los princípios generales de derecho, puedan estos haber tenido reconocimento escrito o no en el marco positivo. Sin perjuicio de lo cual, la ratificación de las convenciones internacionales sobre derechos humanos, así como el reconocimiento de los derechos humanos por su Carta Magna y demás disposiciones jerárquicamente inferiores, proveen de un elace rápido y tangible con aquellos princípios rectores del ordenamiento jurídico[83].

[83]Tradução do pesquisador: "O Uruguai conta com um coerente sistema de proteção dos direitos fundamentais sustentado em uma estrutura jurídica cujo principal pilar está dado por um grupo normativo constituído pelos principios gerais do direito, podem eles ter recebido reconhecimento escrito ou não. Sem prejuízo do qual, a ratificação das convenções internacionais sobre direitos humanos, assim como o reconhecimento da Carta Magna e demais disposiçõesa ela hierarquicamente inferiores, provém de um enlace rápido e tangível com aqueles princípios reitores do ordenamento jurídico."

A legislação uruguaia, assim como a legislação argentina, traz dispositivos com as definições legais. Dentre estas definições, afirma, em seu artigo 4º (URUGUAI, 2014), que dado pessoal significa: "información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables[84]".

Por outro lado, este mesmo dispositivo prevê que dado sensível significa "Datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual[85]." (URUGUAI, 2014)

Estas definições são muito semelhantes àquelas previstas na lei argentina e visam subsidiar o intérprete na compreensão do restante da legislação, visualizando-se que a norma uruguaia também parte da distinção entre dados sensíveis e não sensíveis para regulamentar esta questão.

Constitui-se em "un derecho del titular del dato que se le informe el carácter de sensible del mismo Ello determinará la obligatoriedad o facultad para responder al interrogatorio[86]". (DAPKEVICIUS, 2014).

A caraterização em dados sensíveis irá ocasionar uma distinção no tratamento destas informações que influenciará diretamente no grau de autonomia que será concedido ao responsável pelo banco onde aquela informação pessoal ficará registrada, portanto o titular deve ter conhecimento de que o dado, cujo tratamento esta consentindo é considerado ou não sensível, nos termos da legislação.

E este conteúdo específico da informação concedida pelo usuário – se o dado é ou não sensível – será apresentada a partir da obrigatoriedade ou não do questionário de obtenção da informação, ou da existência de sanção pela recusa.

Outra disposição que merece referência é a que trata da qualidade do dado, ou, como afirma o art. 7º (URUGUAI, 2014), do princípio da veracidade do dado:

> Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley. Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario. Cuando se constate la inexactitud o falsedad de los

[84]Tradução do pesquisador: "qualquer informação relativa a pessoas físicas ou jurídicas identificadas ou identificáveis."

[85] Tradução do Pesquisador: "Os dados pessoais que revelem a origem racial ou étnica, opiniões políticas, crenças religiosas ou morais, filiação sindical e dados relativos à saúde ou vida sexual"

[86] Tradução do Pesquisador: "um direito do titular do dado ser informado do caráter sensível deste dado, sendo este caráter determinante para se identificar a obrigatoriedade ou faculdade de fornecimento do dado."

> datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley[87].

Aqui, de forma semelhante à legislação argentina, a legislação uruguaia também refere qualidades que os dados devem ter, determinando que eles devem ser precisos, adequados, equilibrados e não excessivos em relação à finalidade de sua captação. Além disto, veda claramente a utilização de meios fraudulentos ou desleais para a captação do dado pessoal, o que é salutar especialmente considerando o dever de observar a boa-fé objetiva.

Estas adjetivações representam princípios que regem o sistema de proteção de dados pessoais dentre os quais, a finalidade, a pertinência, também devem ser respeitados, pois essas informações integram o direito de privacidade do titular. Conforme afirma Felipe Rotondo: "Estos principios, conjuntamente con la regulación el bloque de juridicidade de mayor jerarquía; entre los derechos de la personalidad basados en este haz normativo, está el de privacidad y el de la citada protección[88]." (ROTONDO, 2014, p. 9)

Porém a legislação argentina acaba sendo mais abrangente quando refere que a obrigatoriedade de retirar ou corrigir dados imprecisos ou inexatos deve ser estendida a todo e qualquer responsável pelo banco de dados, enquanto que a legislação uruguaia afirma apenas que o controlador terá esta obrigação.

É preciso evidenciar, ainda, que se trata de uma prática empresarial corriqueira a atuação conjunta de diferentes empresas, e nestas situações geralmente apenas uma destas empresas recolhe o consentimento expresso do titular, porém o tratamento dos dados acaba ocorrendo pelas outras.

Deste modo, é importante que a legislação seja abrangente e imponha deveres de cuidado e respeito às finalidades expressas inicialmente, no momento da captação, a todas as pessoas jurídicas incorporadas a cadeia de proteção e tratamento dos dados pessoais.

---

[87] Tradução do Pesquisador: "Os dados pessoais recolhidos para o tratamento devem ser precisos, adequados, equilibrados e não excessivos em relação à finalidade para a qual eles foram obtidos. A coleta de dados pode não não pode occorer por meio desleal, fraudulento, abusivo ou obtido através de violação das disposições desta lei. Os dados devem ser precisos e atualizados, caso seja necessário. Quando a inexatidão ou falsidade das informações for encontrada, o controlador, ao tomar conhecimento de tais circunstâncias deverá excluir, substituir ou suplementar os arquivos para que os dados permaneçam precisos, verdadeiros e atualizados. Além disso, devem ser eliminados dados cujo uso para o qual foram captados já expirou de acordo com as disposições da presente lei"

[88] Tradução do pesquisador: "estes princípios, conjuntamente com a regulação constitucional e com o direito internacional dos direitos humanos, configuram um bloqueio de juridicidade de maior hierarquia."

A legislação uruguaia, no referido dispositivo, não refere nada quanto ao direito do usuário ao acesso aos seus dados pessoais, bem como o seu direito a retificação, supressão ou atualização, diferente do que consta expressamente prevista na legislação argentina.

Neste ponto, a legislação uruguaia acaba tornando mais vulnerável a personalidade individual dos titulares dos dados pessoais, pois não refere, no mesmo dispositivo onde elege as características que os dados arquivados deverão ter, que estes deverão ser retificados, suprimidos ou atualizados conforme requerimento do titular.

Outro dispositivo é o artigo 8º (URUGUAI, 2014), referente à finalidade da captação e estabelece:

> Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Los datos deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya permitido tal necesidad o pertinencia. Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular[89].

Aqui a preocupação da legislação uruguaia cinge-se ao critério temporal, ou seja, exige do responsável que verifique se a finalidade para qual foi captado o dado pessoal ainda persiste. Deste modo, a lei demonstra claramente que o dado pessoal pode, pelo transcurso de um determinado tempo, perder a sua finalidade, quando deverá ser imediatamente removido dos bancos de dados.

Porém, a legislação traz uma exceção para dados que tenham valor histórico, estatístico ou científico, pois nestes casos é permitida a sua manutenção, mesmo após a sua finalidade estar desatualizada, sendo que a legislação argentina não refere nada precisamente quando ao critério cronológico, tão pouco a sua exceção.

Esta previsão de que, cronologicamente, quando um determinado dado não cumprir mais a sua finalidade, não mais será utilizado, garante a eficácia da autodeterminação informativa, pois o titular, quando der o seu consentimento, estará também determinando quando aquele dado deve ser eliminado.

---

[89] Tradução do Pesquisador: "Dados processados não podem ser utilizados para fins diferentes ou incompatíveis com as finalidades para as quais foram obtidos. Os dados devem ser removidos quando não são mais necessários ou relevantes para os fins para os quais eles poderiam ter sido recolhidos. As regras e procedimentos a determinar os casos em que, por exceção, e participou do valor histórico, estatísticos ou científicos, e de acordo com a legislação específica, a informação pessoal é mantida, mesmo que tal necessidade esteja desatualizada ou irrelevante. Também não pode comunicar dados entre bancos de dados sem que seja lei ou consentimento prévio informado do proprietário."

Como afirma o autor uruguaio Rotondo (2014, p. 9):

> En suma son aplicables los criterios de finalidad y proporcionalidad; procede efectuar una apreciación de idoneidad, de necesidad y de proporcionalidad, este último en el sentido estricto de ponderación, para legitimar la comunicación, lo que importa especialmente cuando esta se hace en base a norma legal que se dicte por razones de interés general[90].

Aqui há uma previsão de que não pode haver comunicação de dados entre diferentes bancos sem previsão legal ou consentimento prévio e informado do titular do dado, o que evita uma eventual segmentação ilícita a partir de tais dados.

Contudo há uma exceção concernente na possibilidade de haver comunicação de dados pessoais entre diferentes entes, mesmo sem o consentimento quando autorizado por lei, porém, neste ponto, a legislação uruguaia padece da mesma omissão que a legislação argentina, pois não fixa limites ou objeto desta lei que possibilitará a transferência entre diferentes bancos de dados.

Além da veracidade e da finalidade, a legislação uruguaia também refere um princípio denominado de consentimento prévio, informado no artigo 9º (URUGUAI, 2014):

> El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 12 de la presente ley. No será necesario el previo consentimiento cuando: A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación. B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma. D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento. E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico[91].

---

[90]Tradução do pesquisador: "Em suma são aplicáveis os critérios de finalidade e proporcionalidade, e assim se deve proceder a uma apreciação de idoneidade, de necessidade e de proporcionalidade, esta última em sentido estrito de ponderação para legitimar a comunicação. Estes critérios são importantes, especialmente quando se está em face de uma norma legal criada por razões de interesse geral"

[91] Tradução do pesquisador: "O tratamento de dados pessoais é lícito, desde que o titular tenha dado o seu prévio consentimento, livre e informado, que deve ser documentado. O referido consentimento dado com outras declarações devem aparecer de forma explícita e em circulação, mediante aviso aos dados necessários, as informações descritas no artigo 12 desta lei. A anuência prévia não é necessária quando: A) Os dados provêm de fontes públicas, tais como registros ou publicações em mídia de massa. B) Foram coletados para o exercício das funções próprias de agências de governo ou em decorrência de uma série de obrigações legais. C) No caso de listagens onde os dados são limitados no caso de indivíduos com nome, identidade, nacionalidade, endereço e data de nascimento. No caso de pessoas coletivas, o nome da empresa, marca, registro único contribuinte, endereço, telefone e identidade das pessoas responsáveis por isso. D) decorrentes de uma relação contratual,

Surge a necessidade do consentimento prévio, livre e informado. Assim como na legislação argentina, este consentimento necessariamente deve ser documentado e, da mesma forma como naquele sistema, deve estar disponível de maneira explícita e em circulação, portanto, ligado ao dado pessoal. Esta previsão privilegia os deveres da informação, da confiança e da lealdade, decorrentes da boa-fé objetiva, pois o internauta deverá confiar que o consentimento documentado expressamente será respeitado quando do tratametno dos seus dados pessoais.

As exceções são muito semelhantes àquelas da legislação argentina, porém com algumas distinções. Na Argentina os dados obtidos por fontes de livre acesso não necessitam de consentimento, porém no Uruguai esta exceção exige que os dados estejam em mídias de massa, o que reduz o âmbito de aplicação desta exceção.

Outra distinção refere-se a última exceção constante na legislação uruguaia, que afirma ser desnecessário o prévio consentimento quando o tratamento é feito por ente singular ou coletivo exclusivamente para o seu uso pessoal ou doméstico. Nesta previsão a lei uruguaia estendeu excessivamente o âmbito de aplicação da exceção, referente ao "uso doméstico".

Não se está a afirmar que necesariamente a legislação deveria adentrar em previsões minuciosas sobre todas as hipóteses possíveis de aplicação, visto que isto prejudicaria a sua própria efetividade para tratar de um tema em constante evolução e que ainda sofre um momento de transição, com o desenvolvimenteo de novas TIC.

Porém como se trata de uma exceção a uma regra que protege direitos fundamentais, exige-se que o intérprete não amplie excessivamente o seu alcance, sob pena de tornar a regra geral que veda o tratamento não consentido de tais dados uma exceção. Portanto seria salutar que a legislação, ao menos quando traz esta exceção, especificasse o conceito do uso doméstico, ou definisse este termo no dispositivo anterior que trata das definições, o que não o fez.

Ainda, esta última exceção não referiu como funcionaria a transmissão de dados utilizados exclusivamente para uso pessoal, sequer afirmou se esta transmissão também deverá ser consentida pelo titular. Quanto a esta exceção do uso exclusivamente pessoal Rubén Flores Dapkevicius (2014) alerta que:

---

científica ou profissional, o titular dos dados, e sejam necessários para o seu desenvolvimento ou implementação. E) O tratamento é feito por ente singular ou coletivo, público ou privado, exclusivamente para seu uso pessoal ou doméstico."

> Sería interesante preguntarse la finalidad de la base doméstica que supo poseer el fundador del F.B.I. Por ello toda base personal doméstica debe adecuarse a la finalidad y pertinencia . No se nos escapa que lo sancionable es la utilización indebida (con fines no domésticos exclusivamente), y que es el uso público el que puede ocasionar la lesión[92].

Exceções extremamente amplas acabam por reduzir o âmbito de aplicação do princípio da exigência de consentimento e, da mesma forma, tendem a abrir brechas ao controle por parte dos usuários, o que enfraquece a sua autodeterminação informativa.

A proteção de dados pessoais constitui-se em um direito fundamental dos indivíduos, e os princípios que visam subsidiar a proteção desse direito devem ser respeitados. Isto somente poderá ocorrer quando as exceções forem interpretadas de forma estrita.

Como afirma Rubén Flores Dapkevicius (2014),"Los principios enumerados, como principios generales, según la ley, son el bloque esencial del instituto de protección de datos. Por ser principios generales sus excepciones deben surgir de texto expreso y son de interpretación estricta que no admite interpretaciones analógicas ni extensivas[93]"

Assim o âmbito doméstico previsto da referida exceção deve necessariamente receber uma interpretação restritiva, pois esta é a única forma de garantir a efetividade do princípio da necessidade de prévio consentimento livre e informado para o tratamento de dados pessoais.

O conteúdo da informação que deve ser fornecido ao usuário no momento do seu consentimento encontra-se na previsão no art. 13 (URUGUAI, 2014):

> Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca: A) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatários. B) La existencia de la base de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable. C) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles. D) Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud. E) La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos[94].

---

[92] Tradução do pesquisador: "Seria interessante perguntar o objetivo da base doméstica que conhecia o próprio fundador do FBI. Portanto, toda base pessoal doméstica deve ser adequada à finalidade e relevância. Não se escapa de tratar e sancionar a utilização indevida (com fins não domésticos exclusivamente), pois é o uso público que poderá ocasionar lesões aos titulares."

[93] Tradução do pesquisador: "Os princípios listados como gerais, de acordo com a lei, constituem-se em um Instituto essencial de proteção de dados. Como princípios gerais, as exceções devem surgir a partir de linguagem explícita e são de interpretação estrita, que não suporta interpretações analógicas ou extensas."

[94] Tradução do pesquisador: "Quando dados pessoais são coletados, os titulares devem ser previamente informados de forma explícita, precisa e inequívoca: A) A finalidade para a qual serão tratados e que podem ser os destinatários ou categorias de destinatários. B) A existência do banco de dados, eletrônico ou não, em questão, a identidade e o endereço do responsável. C) O carácter obrigatório ou facultativo das respostas ao questionário que é proposto, especialmente no que diz respeito a dados sensíveis. D) As consequências do fornecimento dos dados e da recusa a fazê-lo ou imprecisão. E) A capacidade do titular para exercer os direitos de acesso, retificação e supressão de dados."

As previsões são muito semelhantes à legislação argentina, sendo que a única distinção seria a referência aos dados sensíveis, afirmando que o caráter das respostas, se obrigatório ou facultativo, será informado especialmente quanto a eles, o que demonstra uma preocupação com a especial proteção que os dados desta natureza exigem.

Para Rubén Flores Dapkevicius (2014), esta referência ao dado sensível seria completamente desnecessária, pois quando se informa ao titular a respeito da possibilidade de ele negar-se a responder, verifica-se claramente esta situação. Porém tal exigência seria conveniente, pois reforça a necessidade de que os dados desta categoria recebam uma maior proteção.

Outra previsão seria o direito ao acesso, previsto no art. 14 (URUGUAI, 2014):

> Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico. Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo, corresponderá a cualesquiera de sus sucesores universales, cuyo carácter se acreditará por la sentencia de declaratoria de herederos. La información debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. Vencido el plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedará habilitada la acción de habeas data. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin[95].

[95] Tradução do Pesquisador: "Os titulares terão direito de obter de cada detentor dos dados pessoais, com identificação prévia, através da identidade ou procuração, todas as informações sobre si mesmo em bancos de dados públicos ou privados. O direito de acesso pode ser exercido gratuitamente no intervalos de seis meses, a menos que seja levantado um interesse legítimo em conformidade com a lei. No caso de dados de pessoas falecidas, o exercício dos direitos a que se refere este artigo será atribuído a qualquer dos seus sucessores universais, cujo caráter é creditado pelo juízo da declaração de herdeiros. As informações devem ser fornecidas no prazo de cinco dias úteis após ter sido solicitado. Após esse período, sem a ordem estar satisfeita ou se negada por razões não justificadas nos termos desta Lei, será habilitado *habeas data*. As informações devem ser fornecidas de forma clara, livre de codificações e se for acompanhado de uma explicação em conhecimento leigo da população média dos termos utilizados. A informação deve ser abrangente e lidar com todo o registro pertencente ao proprietário, mesmo que o único requisito para compreender um aspecto de dados pessoais. Em qualquer caso, o relatório pode divulgar os dados pertencentes a terceiros, mesmo quando ligado a essa pessoa. A informação, à escolha do titular, pode ser prestada por escrito, por, telefone, imagem eletrônica ou outro adequado para este fim."

Nota-se que a previsão do direito ao acesso na legislação uruguaia, ao contrário da legislação argentina, autoriza expressamente que o titular outorgue uma procuração para terceiro ter acesso aos seus dados pessoais que estejam arquivados em bancos de dados, públicos ou privados.

Assim como na legislação argentina, a legislação uruguaia também estabelece um limite temporal de seis meses para o exercício gratuito do acesso aos dados pessoais, pelo que persiste a crítica sobre tal procedimento, já feita anteriormente.

Quanto à transmissão do direito ao acesso aos herdeiros, há uma exigência de que este caráter seja creditado pelo juízo da declaração de herdeiros, que não é prevista na legislação argentina. Este condicionamento consistirá em um empecilho ao exercício do direito ao acesso pelos herdeiros, pois aqueles que ainda não foram creditados, mas desejam acessar dados do de *cujus*, não poderão fazê-lo.

Outra distinção em face da legislação argentina é que o prazo para o fornecimento das informações ficou reduzido para cinco dias úteis, o que se mostra uma medida salutar, pois a necessidade de acesso para o proprietário ou titular do dado que intenta este procedimento geralmente não prescinde de urgência.

Após o prazo, o titular ficará habilitado para impetrar a ação de *Habeas Data*, porém, assim como afirmado quando do comentário anterior à legislação argentina, este procedimento prévio pode significar um empecilho ao exercício do direito ao acesso, pois não se trata de um direito integralmente gratuito, no caso do dado arquivado a mais de seis meses.

As demais previsões quanto ao direito ao acesso são muito semelhantes à legislação argentina, pelo que os comentários a ela feitos se estendem à presente legislação uruguaia.

Outra questão significativa que a legislação uruguaia prevê refere-se aos demais direitos decorrentes do acesso aos dados pessoais, ou seja, as prerrogativas de retificação, atualização, inclusão ou supressão, todos previstos no art. 15 (URUGUAI, 2014):

> Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular. El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde. El incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del

> plazo, habilitará al titular del dato a promover la acción de habeas data prevista en esta ley[96].

A legislação uruguaia previu de forma muito semelhante à legislação argentina, porém, ao contrário desta, deixou de contemplar a possibilidade de o titular do dado pessoal atribuir a ele o status de confidencialidade.

A confidencialidade é importante, pois muitas vezes o titular não pretende que determinado dado pessoal seja necessariamente suprimido, apenas gostaria que determinadas informações a seu respeito passassem a ter um grau maior de discrição.

Outra distinção foi que a legislação uruguaia atribui a responsabilidade pela retificação e demais situações ao chefe do banco de dados ou o processador, enquanto que a legislação argentina previu que qualquer usuário do banco de dados deve proceder à retificação. Esta amplitude dos obrigados a cumprir o dever de retificação torna a legislação argentina mais protetiva, visto que muitas vezes o pedido ou a constatação do equívoco ocorre com outro usuário que não necessariamente o chefe ou processador[97].

Os dados sensíveis também receberam uma especial proteção da legislação uruguaia, conforme previsto no artigo 18 (URUGUAI, 2014);

> Ninguna persona puede ser obligada a proporcionar datos sensibles. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares. Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato. Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u outorgare. Nada de lo establecido

[96] Tradução do Pesquisador: "Qualquer pessoa singular ou coletiva tem o direito de solicitar a correção, atualização, inclusão ou exclusão de dados pessoais, que corresponde incluídos em um banco de dados, que foram encontrados erro ou falsidade ou exclusão das informações que possuem. O chefe do banco de dados ou o processador deve proceder a correção, atualização ou exclusão, incluindo através das operações necessárias para o efeito no prazo máximo de cinco dias úteis após a recepção do pedido por parte do proprietário dos dados ou, se for o caso, comunicar as razões porque não considera aplicável. Violação desta obrigação pelo responsável pelo banco de dados ou o tratamento ou a data de vencimento, permitirá que o titular dos dados promova a ação de *habeas data*, previstos na presente lei."

[97] As demais previsões são semelhante à legislação argentina, pelo que os comentários lá feitos se aplicam a legislação uruguaia também.

> en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren conveniente[98].

O tratamento dos dados sensíveis apresenta-se muito semelhante da legislação argentina, ou seja, em regra veda o recolhimento e o tratamento dos dados desta natureza sem o prévio consentimento por escrito, livre e informado do seu titular.

Uma distinção é que a legislação argentina trata apenas da questão do interesse geral autorizado por lei, como exceção a esta vedação, o que já é criticável pela imprecisão do significado do termo "interesse geral", enquanto que a legislação uruguaia refere que também pode haver recolhimento e tratamento de dados sensíveis quando a organização requerente tem um mandato legal para fazê-lo, o que amplia excessivamente esta exceção, tornando esta regra praticamente inócua.

A legislação uruguaia não foi capaz de delimitar o significado do termo "interesse geral autorizado por lei", o que já enfraquece a proteção aos dados pessoais dos usuários. Porém esta garantia torna-se praticamente ineficiente, quando esta possibilita que determinados órgãos[99] recebam um mandato legal para recolher e tratar dados pessoais sensíveis sem referir a finalidade.

Esta possibilidade de tratamento de dados sensíveis, sem o consentimento do titular quando o responsável está no exercício de um mandato legal, denota a situações de vigilância e controle, alertadas por Stefano Rodotá (2008).

Contudo a legislação uruguaia demonstra uma precisão maior que a legislação argentina quando refere a exceção à vedação baseada em alguns detentores específicos dos dados – partidos políticos, associações, Igreja Católica, dentre outros –, pois afirma que a obtenção dos dados sensíveis, nestes casos, deve ocorrer por motivos políticos, religiosos, associativos, dentre outros, que se relacionam às atividades essenciais dessas pessoas jurídicas.

---

[98] Tradução do Pesquisador: "Nenhuma pessoa pode ser obrigada a fornecer dados sensíveis. Estes só podem ser processados com o expresso consentimento por escrito do proprietário. Os dados sensíveis só podem ser recolhidos e tratados por razões imperiosas de interesse geral, autorizadas por lei, ou quando a organização requerente tem um mandato legal para fazê-lo. Eles também podem ser tratados com fins estatísticos ou científicos, quando desassociar dos seus titulares. É proibida a formação debanco de dados para armazenar informações que revelem direta ou indiretamente, os dados sensíveis. As exceções são aqueles que detêm os partidos políticos, sindicatos, igrejas, denominações, associações, fundações e outras organizações sem fins lucrativos cujo objetivo é político, religioso, filosófico, associação, referindo-se à origem racial ou étnica, saúde e sexualidade, como para os detalhes de seus parceiros ou membros, sem prejuízo da divulgação dos dados, que requerem sempre o consentimento prévio dos usuários."

[99] Dentre estes órgão é possível exemplificar as forças armadas de uma determinada nação, ou mesmo as forças responsáveis por segurança pública, dentre outras.

Além disto, a legislação uruguaia afirma expressamente que esta exceção aplica-se somente a entidades sem fins lucrativos, referência não existente na legislação argentina. Outra questão é que, mesmo no caso desta exceção, a divulgação dos dados por estas entidades sempre irá exigir consentimento prévio e informado dos titulares destes dados. Contudo a mera garantia do direito ao acesso e dos conseguintes direitos dele decorrentes ao titular por si só não garante que ele possa realmente fazer valer tais direitos.

Para tanto se torna necessária a previsão de uma ação específica com tal finalidade, como faz a lei uruguaia no artigo 37 (URUGUAI, 2014):

> Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso[100].

A ação, de forma semelhante à lei argentina, deverá ser intentada pelo titular do dado pessoal em face do ente que detém a referida informação. Esta ação poderá ter como objetivo tanto garantir o acesso como possibilitar a retificação daqueles dados pessoais, em caso de erros ou falhas.

Assim esta ação se trata de (DAPKEVICIUS, 2014) "un proceso contencioso y sumario ya que su objeto es la defensa de derechos que pueden ser destruidos en cuestión de horas. Por ello se estructuró un juicio brevísimo donde se dilucide con la mayor profundidad posible el derecho cuestionado[101]."

O que a lei uruguaia refere, ao contrário da lei argentina, que silencia quanto à matéria, é que, em determinados casos em que a norma legal determine que tal dado deva ser mantido em segredo, o juiz deverá levar esta condição em conta quando da apreciação da ação. Tal situação ocorre, por exemplo, com os registros bancários e fiscais, que têm leis específicas que os regulamentam, e que determinam o seu segredo.

---

[100] Tradução do Pesquisador: "Toda a pessoa terá direito a intentar uma ação judicial efetiva para tomar conhecimento dos dados referentes à sua pessoa e a finalidade de sua captação e tratamento, que constem em bases de dados públicas ou privadas, e em caso de erro, falsidade, proibição de tratamento, discriminação ou desatualização, exigir sua retificação, inclusão ou supressão ou que entender pertinente. Quando se trate de dado pessoal cujo registro está amparado por uma norma legal que consagre o respeito ao segredo, o juiz apreciará o tratamento dele em atenção às circunstâncias do caso concreto."

[101] Tradução do Pesquisador: "processo contencioso e sumário, já que seu objeto será exclusivamente a proteção de um direito que poderá ser destruído em questão de horas. Por isso se estruturou um juízo sumário onde se decide com a maior brevidade possível o direito questionado."

A lei uruguaia ainda afirma, quanto aos polos da referida ação, nos artigo 38 (URUGUAI, 2014):

> El titular de datos personales podrá entablar la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos: A) Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley. B) Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley. Serán competentes para conocer en las acciones de protección de datos personales o habeas data: 1) En la capital, los Juzgados Letrados de Primera Instancia en lo Contencioso Administrativo, cuando la acción se dirija contra una persona pública estatal, y los Juzgados Letrados de Primera Instancia en lo Civil en los restantes casos. 2) Los Juzgados Letrados de Primera Instancia del Interior a quienes se haya asignado competencia en dichas matérias[102].

O procedimento prévio e extrajudicial, seja de acesso, retificação, supressão ou atualização, aparece como um pressuposto para o ajuizamento da ação judicial, o que poderia prejudicar o seu correto exercício. Porém, de forma semelhante à lei argentina, em caso de o responsável deixar de obedecer ao pedido dentro do prazo, a parte poderá diretamente intentar a ação judicial.

Ainda, quanto aos legitimados, o artigo 39 (URUGUAI, 2014) prevê:

> La acción de habeas data podrá ser ejercida por el propio afectado titular de los datos o sus representantes, ya sean tutores o curadores y, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado. En el caso de personas jurídicas, la acción deberá ser interpuesta por sus representantes legales o los apoderados designados a tales efectos[103][104].

Quanto a estas regras de legitimidade, Rubén Flores Dapkevicius (2014) afirma que:

---

[102] Tradução do Pesquisador: "O titular dos dados pessoais pode ajuizar ação para a proteção de dados pessoais ou *habeas data* contra todos responsáveis por uma base de dados pública ou privada, obedecendo as seguintes premissas: A) Quando quiser saber os seus dados pessoais que estão registrados em um banco de dados ou as informações de como e tal foi negado, ou não tenha sido fornecido pelo responsável pelo banco de dados, conforme as previsões e limites desta lei. B) Quando solicitado ao chefe do banco de dados retificação, atualização, eliminação, adição ou remoção, e este não o tenha feito no prazo legal ou tenha apresentado razões insuficientes para deixar de fazê-lo."

[103] Tradução do Pesquisador: "A ação de *habeas data* poderá ser exercida pelo proprietário dos dados em questão, seus representantes, ou encarregados de educação e, se pessoas mortas, por seus sucessores universais em linha reta ou colateral até o segundo grau, pessoalmente ou por procuração. No caso de pessoas coletivas, a ação deve ser apresentado por seus representantes legais ou responsáveis designados para o efeito."

[104] Outras questões processuais previstas nos arts. 40 a 45 da lei uruguaia não diferem da legislação argentina, além de não trazerem grande contribuição à temática aqui tratada, por isso estas previsões não serão objeto de comentários.

> Los sujetos legitimados activos en la acción son el titular de los datos, aún fallecido y sus representantes. El legitimado pasivo lo será el responsable de la base de datos, más allá de los eventuales citados en garantía y otros posibles responsables como los cesionarios y encargados de datos, etc.[105]

Por fim, a última questão relevante a ser tratada será a do órgão de controle previsto na lei uruguaia no art. 31 (URUGUAI, 2014): "Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales[106]."

Esta agência funcionará assistida por um conselho consultivo formado por cinco membros provenientes do Poder Judiciário, do Ministério Público, da área acadêmica, do setor privado e pelo próprio presidente da AGESIC, que será o seu presidente, tudo conforme previsão do art. 32 (URUGUAI, 2014).

Porém a previsão mais relevante da legislação uruguaia quanto a este órgão de controle se refere a suas atribuições e competências que estão previstas no art. 34 (URUGUAI, 2014):

> El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: A) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza. B) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley. C) Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos. D) Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes. E) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados. F) Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta. G) Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a protección de datos personales.

---

[105] Tradução do Pesquisador: "Os legitimados ativos são os titulares dos dados e, caso falecidos,por seus sucessores. E os legitimados passivos serão os responsáveis pela base de dados, porém esta legitimidade deve ser estendida como garantia aos titulares, a qualquer outro ente possivelmente responsável, como os cessionários, gerentes, e usuários, dentre outros"

[106] Tradução do Pesquisador: "Fica criado uma Agência de Controle descentralizada para o Desenvolvimento do Governo Eletrônico e Sociedade da Informação e do Conhecimento (AGESIC), dotado com o corpo mais completa autonomia técnica, a Unidade de Regulação e Controle Dados Pessoais [...]"

> H) Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita[107].
>
> .

Este órgão de controle tem funções semelhantes ao órgão constante na legislação argentina, porém com algumas distinções de relevância, como o fato de ser responsável por ajudar o Poder Executivo na criação de projetos de lei sobre a proteção de dados pessoais, considerando que ele seria órgão com maior experiência neste assunto.

Além desta função, este órgão tem a prerrogativa de, gratuitamente, informar a qualquer pessoa sobre a existência de seus dados em bases de dados pessoais, sua finalidade e identidade dos responsáveis, atribuição que não aparece expressa na lei argentina.

Por outro lado, a lei argentina concedeu ao órgão de controle inclusive competência em matéria criminal, algo que a legislação uruguaia não o fez expressamente. A atribuição de tal competência geraria um maior poder de coerção deste órgão em face dos entes que realizam o tratamento de dados pessoais.

Como afirma Felipe Rotondo (2014, p. 10), exemplificando as funções deste importante órgão:

> Este órgano, creado por la ley 13.331, se ha pronunciado sobre casos de comunicación de datos entre entes estatales, especificamiente respecto de proyetos de convênios o de norma sobre dicha temática. Tuvo en cuenta la finalidade de la mejora de la gestión de los entes intervenientes y la aplicación del principio de finalidade, motivo por el cual destaco que los datos no se deben utilizar para fines distintos de aquellos para los que fueron recabados, de manera tal que "las bases de la información orignales intercambiadas" no pueden ser de libre uso, como se proponía en el convenio[108].

---

[107] Tradução do Pesquisador: "O órgão de fiscalização realizará todas as ações necessárias para cumprir os objetivos e outras disposições da presente lei. Para este efeito, terá as seguintes funções e competências: A) Para ajudar e aconselhar as pessoas que necessitam sobre o escopo da presente lei e os meios legais disponíveis para defender os direitos nele garantidos. B) A emitir regras e regulamentos a serem observados no desenvolvimento das atividades abrangidas pela presente lei. C) Realizar um banco de dados do censo feito pela lei e manter um registro permanente deles. D) Monitorar o cumprimento das regras sobre a integridade, precisão e segurança dos dados por parte dos responsáveis dos bancos de dados, tais efeitos podem tomar as ações de inspecção em causa. E) Pedir mais informações a entidades públicas e privadas, que por sua vez devem fornecer os registros, documentos, programas ou outros itens relativos ao tratamento de dados pessoais. Nesses casos, a autoridade deve garantir a segurança e confidencialidade dos elementos de informação fornecida. F) Emitir parecer sempre que for solicitado pelas autoridades competentes, incluindo os pedidos de emissão de sanções administrativas em caso de violação das disposições da presente lei, os regulamentos ou resoluções que regulam o tratamento de dados pessoais incluída na mesma. G) Conforme exigido, assessorar o Executivo sobre a apreciação dos projetos de lei que se relacionam no todo ou em parte, para a proteção dos dados pessoais. H) Informar qualquer pessoa sobre a existência de bases de dados pessoais, a sua finalidade e a identidade dos responsáveis, de forma gratuita"

[108] Tradução do pesquisador: "Este órgão, criado pela lei 18.331, tem se pronunciado sobre casos de comunicação de dados entre entes estatais, especificamente a respeito de projetos de convênios ou de normas sobre a temática. Tem como uma finalidade a melhora da gestão dos entes intervenientes, motivo pelo qual destacou que os dados não devem ser utilizados para fins distintos daqueles para os quais foram recolhidos, de modo que as bases de informação originais não podem ser de livre uso, como já se propôs em um convênio"

A legislação uruguaia em muitos aspectos consegue ser mais protetiva que a legislação argentina, talvez por ser uma legislação posterior que já teve a oportunidade de recolher diversas experiências daquela legislação. Dentre estes pontos, sem dúvida o que merece uma referência expressa é a predisposição em elencar quais são os princípios que formam o núcleo duro de proteção dos dados pessoais, ao contrário da legislação argentina, onde estes princípios são extraídos das disposições.

Contudo a legislação do Uruguai tornou-se menos protetiva em muitos outros aspectos, como na questão da atribuição de responsabilidade para retificações, onde limita esta responsabilidade apenas ao chefe ou controlador. Outra questão é o acréscimo de uma exceção extremamente vaga e ambígua ao princípio da exigência de prévio consentimento, na hipótese da utilização de bancos de dados para uso doméstico.

2.2.3 O tratamento do tema no Brasil: o Marco Civil da *Internet* e o Projeto de Lei da Proteção de Dados Pessoais.

Antes de adentrar propriamente na análise das previsões do Marco civil em conjunto com as possíveis previsões do projeto de proteção de dados pessoais, torna-se essencial delimitar objetivamente a abordagem que será feita.

Não haverá especificamente o estudo da garantia fundamental do *Habeas Data*, que nos outros países analisados foi objeto da mesma lei de proteção de dados pessoais, e que no Brasil foi regulamentada inicialmente em nível constitucional, com o art. 5º inciso LXXII da Constituição Federal de 1988 (BRASIL, 2014), e após através da Lei 9.507 de 12 de novembro de 1997.

Estas previsões não visam ao acesso aos bancos de dados digitais. Na realidade a garantia constitucional do *Habeas Data* no Brasil surgiu como resposta a um período de ditadura militar que praticou inúmeros ilícitos contra os direitos humanos, e onde as vítimas e seus familiares pretendiam o acesso aos bancos de dados públicos para ter conhecimento dos autores destes ilícitos (MENDES; BRANCO, 2014, p. 564). Esta visão é corroborada pela própria delimitação constitucional de que o acesso que se pretende obter com tal medida judicial objetiva o banco de dados público ou de caráter público[109].

Portanto, pela delimitação específica, bem como pelo contexto histórico de seu surgimento, esta ação constitucional não será objeto específico de análise, que se limitará

[109] A Lei nº 9.507 de 1997, estabelece, em seu art. 1º, parágrafo único que "considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações."

apenas à Lei nº 12.965/2014 no que tange aos dados pessoais e ao arquivado Anteprojeto de Lei de Proteção de Dados forem omissas, como no caso do direito ao acesso, e do seu decorrente direito à retificação.

É preciso compreender que houve uma iniciativa de normatização da proteção de dados pessoais no Brasil por meio do Projeto de Lei nº 4.060 de 2012[110] que, segundo sua ementa, "Dispõe sobre o tratamento de dados pessoais, e dá outras providências." (BRASIL, 2014-b).

Este projeto de relatoria do Deputado Nelson Marchezan Junior (PSDB-RS) foi remetido em 21 de Agosto de 2013 para a Comissão de Ciência e Tecnologia, Comunicação e Informática – CCTCI da Câmara dos Deputados, onde aguardou tramitação até 31 de Janeiro de 2015, quando os parlamentares optaram por arquivá-lo (CAMARA DOS DEPUTADOS, 2015).

Tal arquivamento deve-se a abertura de uma consulta pública[111] pelo Ministério da Justiça em 28 de Janeiro de 2015 com o objetivo de regulamentar o Marco Civil da Internet e de produzir um novo Anteprojeto de Lei de Proteção de Dados. No mesmo ato foi nomedo o professor Danilo Doneda para compor um grupo de trabalho que irá, com o apoio das consultas populares, elaborar um novo texto.

Portanto, atualmente no Brasil, as únicas previsões de proteção de dados pessoais no ambiente virtual que efetivamente estão em vigor constam da Lei nº 12.965, de 23 de Abril de 2014 que, segundo sua ementa, "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014-a).

Tal legislação ficou conhecida como o Marco Civil da *Internet*, pois foi a primeira previsão de caráter geral que especificamente pretendeu regulamentar a utilização destas tecnologias no território nacional.

Para que os objetivos e razões que motivaram a criação do Marco Civil fiquem corretamente delimitados, é essencial compreender "A importância do espaço virtual na interligação entre as pessoas, possibilitando o exercício dos seus direitos, impõe a necessidade de uma disciplina jurídica aplicável a esta plataforma mundial, estabelecendo igualmente os deveres existentes nesse espaço." (AZEVEDO, 2014, p. 90)

---

[110] Como já informado em nota anterior tal projeto de lei foi arquivado em 31 de Janeiro de 2015, conforme informação constante no dite da Câmara Federal. (CÂMARA DOS DEPUTADOS, 2015), e como já visto o Ministério da Justiça abriu em 28 de janeiro de 2015, consulta pública para a elaboração de um novo anteprojeto. (BLOG DO PLANALTO, 2015).

[111] O ordenamento jurídico brasileiro já vivenciou esta experiência com o Marco Civil da Internet cujo anteprojeto de lei também surgiu a partir de uma consulta pública, que além de tratar-se de uma metodologia legislativa mais democrática, tem o mérito de qualitativamente produzir um texto mais adequado à realidade social, sobretudo uma realidade com um alto nível de transformação como no caso da sociedade informacional.

O Marco Civil buscou delimitar o tratamento jurídico da *Internet* e além de prever uma série de princípios gerais, estabeleceu diversos direitos e deveres dos envolvidos com a rede, e tratou de temáticas de naturezas diversas, partindo da questão da relação entre o Estado e os usuários da rede, regulamentando as obrigações dos provedores de acessos e referindo a proteção de dados pessoais.

Para entender esta legislação é essencial compreender o seu histórico:

> Em 2009, a Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, iniciou uma série de discussões públicas para a apresentação de um projeto colaborativo de lei que pudesse regular o uso da Internet no Brasil, estabelecendo princípios e garantias dos usuários da rede e delimitando a atuação do Estado nesse setor – iniciativa esta que se tornou conhecida como Marco Civil da Internet [...] Em 2011, o Marco Civil foi apresentado à Câmara dos Deputados como o Projeto de Lei n. 2.126/2011, contendo 25 artigos que tratam de temas como responsabilidade civil, guarda de registros de conexão, retirada de conteúdo e neutralidade da rede. No fim de 2012, foram realizadas uma nova rodada de debates online promovidos no site www.edemocracia.camara.gov.br e diversas audiências públicas, com o objetivo de discutir os temas do Marco Civil junto à comunidade científica, representantes da sociedade civil e empresas do setor (FERREIRA, 2014, p. 9).

Inicialmente, assim como a Constituição Federal, o Marco Civil da *Internet* estabeleceu diversos fundamentos para a disciplina do uso da *Internet*. Dentre este fundamentos se destacam a "liberdade de expressão", prevista no *caput* do art. 2º. A legislação também estabelece como fundamento "os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais", constante do inciso II, ambos do art. 2º (BRASIL, 2014-a).

Esta previsão, assim como os fundamentos da república previstos na Constituição, pretende esclarecer quais os valores que o sistema de proteção estabelecido pelas legislações sobre a temática da *Internet* terá por objetivo resguardar.

Nestas previsões visualiza-se que a autodeteminação informativa, que decorre dos direitos à liberdade e à dignidade da pessoa humana, também deve ser contemplada pelas legislações, assim, de certa forma, esta previsão visa que as futuras legislações sobre a temática concedam ao titular do dado pessoal maior controle sobre as finalidades de sua aplicação.

Após esta previsão, em seu art. 3º, a legislação estabelece os princípios para a disciplina do uso da *Internet*, dentre os quais são relevantes para a temática da proteção de dados pessoais a "proteção da privacidade", no inciso II, e a "proteção dos dados pessoais, na forma da lei", no inciso III (BRASIL, 2014-a).

Conforme destacam comentaristas desta legislação (JESUS, MILAGRE, 2014, p. 12): "Além de proteger a privacidade em geral, o Marco Civil dá ênfase à proteção dos dados pessoais, informações que podem identificar uma pessoa e que comumente são utilizadas ou requeridas pelos provedores de acesso à *Internet* ou provedores de serviços no Brasil."

Nesta previsão princiológica, destacam-se dois pontos negativos. Inicialmente cinde a proteção à privacidade da proteção aos dados pessoais, o que pode enfraquecer este segundo valor, considerando que ele, na realidade, seria uma nova forma de proteção da privacidade, portanto, melhor seria uma previsão que afirmasse que é um princípio à proteção da privacidade por intermédio da proteção aos dados pessoais. Em um segundo momento, a previsão aparentemente condiciona a proteção específica dos dados pessoais à existência de uma Legislação sobre a temática, quando na realidade ela poderia ter elencado como princípio a mera proteção aos dados pessoais.

Visualiza-se claramente que o Marco Civil pretendeu ter um papel semelhante a uma Constituição para tratar de questões jurídicas envolvendo a *Internet*, pois, quando trata destas questões, remete a legislações específicas, dentre as quais algumas que ainda não existem, como o caso da lei de proteção de dados pessoais.

A experiência mais próxima de uma regulamentação específica da matéria foi o Projeto de Lei nº 4.060 de 2012, em seu art. 7º, inciso I (BRASIL, 2014-b), definia dado pessoal como "qualquer informação que permita a identificação exata e precisa de uma pessoa determinada."

Tal previsão, ao contrário das legislações argentina e uruguaia, pretendia restringir o alcance do termo dado pessoal. Enquanto que nas legislações estrangeiras estudadas havia a previsão de que mesmo informações pertinentes a pessoas determináveis seriam consideradas dado pessoal, no caso brasileiro o recém arquivado projeto previa que somente aquela informação que permitisse a identificação exata de uma pessoa teria esta qualificação.

Esta restrição, se fosse mantida, tornaria prejudicial aos direitos fundamentais do titular dos dados pessoais, pois muitas vezes uma determinada informação por si só não permite a identificação de determinado indivíduo, porém em conjunto com outros dados – como ocorre no caso da segmentação por cruzamento de dados – permite que aquele indivíduo seja identificado. Deste modo, a manutenção dessa definição retiraria do âmbito de controle os dados que indiretamente podem revelar detalhes da personalidade do cidadão, enfraquecendo a sua autodeterminação informativa.

Deve-se referir que a própria legislação do Marco Civil trouxe uma previsão com o intuito de vedar qualquer espécie de filtro de informações decorrentes do acesso, conforme

prevê o § 3º do art. 9º (BRASIL, 2014-a): "Na provisão de conexão à Internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo"

Esta previsão do parágrafo terceiro do art. 9º é uma das previsões que melhor protege a autodeterminação informativa, pois veda ao responsável pelo tráfego de dados a filtragem de informações com o intuito de identificação do acesso do titular.

Como afirmam (JESUS, MILAGRE, 2014, p. 12):

> Não se tinha garantias até o Marco Civil, sobre o que os provedores registravam em relação aos seus usuários. Com a garantia acima prevista, torna-se ilegal aos provedores interferirem na navegação dos usuários ou mesmo conhecer o que os usuários estão a fazer na Internet. Garante-se, com tal disposição, o sigilo das comunicações virtuais e a privacidade do usuário da Internet. Igualmente, assegura ao usuário que ele não terá tráfego preterido ou bloqueado pelo provedor de acesso.

Esta norma, pela forma como está prevista, visa uma prestação de serviços mais transparente entre os provedores e os usuários, porém não objetiva precisamente a proteção à privacidade. Essa constatação é possível a partir das suas lacunas, pois não veda, por exemplo, a cessão destes mesmos dados de conexão a outros entes, cingindo-se aparentemente a uma correta relação contratual, mas não necessariamente a uma precisa proteção de direitos fundamentais.

Outra questão que o Projeto de Lei nº 4.060 de 2012 também pretendia definir é o conceito de dado pessoal sensível. Ele afirma que esta categoria seria pertinente às "informações relativas à origem social e étnica, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular", conforme art. 7º, incico III (BRASIL, 2014-b).

Da mesma forma que o conceito de dado pessoal, a previsão que definiria dado pessoal sensível também limitou excessivamente o alcance da proteção, pois nada refere à suscetibilidade desta espécie de dados causarem discriminação ou não[112].

A razão de existir uma categoria de dados pessoais que recebem um grau de proteção mais elevado e são considerados dados sensíveis é a sua suscetibilidade de causar discriminação. Porém, identifica-se um problema quando a conceituação de dados pessoais sensíveis elenca uma série de exemplos, sem referir que estes não excluem quaisquer outros suscetíveis de causar discriminação. Por exemplo, a legislação não refere nada a respeito dos padrões de consumo, informações que também são suscetíveis de causar discriminação do

[112] Poderia ocorrer interpretação ampliativa desta previsão, porém isto dependeria de uma discricionariedade do intérprete, que poderia ou não tender à proteção aos direitos do internauta.

titular, se ele consome produtos vegetarianos, ou com um baixo grau de reponsabilidade ambiental na sua produção, estas informações podem prejudicar determinados indivíduos. Outro exemplo, não contemplado no rol refere-se às informações pertinentes a procedimentos jurisdicionais que podem prejudicar os titulares das mais diversas formas.

Na realidade a necessidade de uma proteção especial aos dados pessoais sensíveis encontra a sua razão de ser na suscetibilidade destes dados causarem discriminação do seu titular, portanto, sempre que a legislação elenca ou determina especificamente quais são estes dados, sem referir expressamente que a sua escolha decorre da suscetibilidade de causarem discriminação, acaba abrindo uma brecha a sua violação, pois limita o intérprete as espécies de dados lá constantes.

A captação e tratamento ilícito dos dados sensíveis certamente não irão ocorrer sobre origem étnica, posição política, ou mesmo orientação sexual, categorias que potencialmente podem causar discriminação, e cuja proteção consta em outras leis. Na realidade esta coleta irá ocorrer sobre outros dados, que em conjunto ou isoladamente, a depender da forma de tratamento (por exemplo, o número de acessos em determinados *sites)*, irão possibilitar que ocorra a violação aos dados pessoais sensíveis.

A garantia da autodeterminação informativa foi um dos objetivos primordiais da Lei nº 12.965, de 23 de Abril de 2014 (Marco Civil da *Internet*), tal constatação decorre do rol de direitos dos usuários previstos no art. 7º (BRASIL, 2014-a), cujo *caput* determina que "acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguinte s direitos"

Conforme o inciso I, o primeiro direito seria a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação". Desta forma:

> Embora a proteção à intimidade e à vida privada esteja prevista na Constituição Federal, em seu art. 5º, inc. X, o Marco é a primeira lei infraconstitucional que regulamenta o tema e bem esclarece ser cabível indenização por dano moral ou material decorrente de violações à intimidade e vida privada no âmbito da Internet[113]. (JESUS, MILAGRE, 2014, p. 18)

A referida previsão tem a sua importância, visto que as indenizações por violação de direitos fundamentais ocorridas no ambitente virtual ainda encontram resistência na comunidade jurídica brasileira, sobretudo pelas dificuldades que existem na localização dos

[113] E essencial referir que a legislação brasileira nos arts. 20, 186 e 187 do Còdigo Civil (BRASIL, 2014-e) já previa a possibilidade de indenizações, porém não especificamente questões envolvendo as TIC como o fez o Marco Civil da Internet.

responsáveis. Porém a proteção à privacidade somente ocorrerá se a autodeterminação informativa for garantida aos titulares dos dados pessoais, como decorrência da nova feição assumida pela privacidade na sociedade informacional (RODOTÁ, 2008).

Outros direitos fundamentais dos usuários consistem na "inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei", conforme inciso II, e na "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial", conforme inciso III, ambos do referido art. 7º (BRASIL, 2014-a).

Tais previsões são de suma importância, pois evitam que as comunicações sofram interferência, ou ainda, que os seus registros sejam violados sem prévia ordem judicial, sobretudo considerando que essas comunicações também consistem em dados pessoais dos seus interlocutores. Portanto estas inviolabilidades também podem ser identificadas como exemplos de proteção aos dados pessoais.

Esta ordem judicial, que deverá ocorrer nos termos do art. 22 da mesma legislação (BRASIL, 2014-a), seria semelhante à decisão que autoriza a interceptação das comunicações telefônicas ou por meios telemáticos, e terá como pressuposto básico a proporcionalidade dos prejuízos decorrentes da própria interceptação e do ilícito que a decisão busca identificar.

Outro direito do titular que merece uma referência expressa refere-se ao "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei", conforme inciso VII do art. 7º (BRASIL, 2014-a).

Esta previsão tende a alterar a política de utilização dos *cookies*, pois, na hipótese dos "banners publicitários [...] o consumidor deverá ser informado que as informação estão sendo coletadas por terceiro, de acordo com artigo 7º, inciso VI do projeto, a página deverá obter o consentimento do internauta para que seja a transferência realizada." (SILVA, 2014, p. 16)

Não havia qualquer previsão neste sentido na legislação brasileira, pois "não tínhamos garantia alguma de que dados que fornecíamos a algum serviço não iriam parar nas mãos de outras empresas ou grupos econômicos, para finalidades diversas." (JESUS, MILAGRE, 2014, p. 19).

Conforme afirma o Deputado Alessandro Molon (2011, p. 39), relator do projeto de lei no Senado Federal:

> Também incluímos dispositivo específico (inciso VIII do art. 7º) com a finalidade de permitir ao usuário o controle sobre suas informações, solicitando a exclusão definitiva de seus dados pessoais, ao término da relação entre as partes, caso entenda conveniente. Buscamos, mais uma vez, explicitar na lei o princípio da

> autodeterminação informativa, atribuindo ao usuário maior controle sobre seus dados pessoais.

Visualiza-se que o princípio do consentimento livre e informado do titular dos dados pessoais surge pela primeira vez na legislação, porém, como não se trata precisamente de uma legislação de proteção de dados pessoais, a forma e condições deste consentimento não constam expressamente neste inciso, relegando-se este papel à futura legislação de Proteção de Dados Pessoais[114].

A dificuldade nesta previsão consiste na forma de prova que o interneuta deverá fazer. Damasio de Jesus e Antonio Milagre (2014, p. 19) esclarecem que a melhor prova seria a "perícia técnica em informática", mas, em qualquer caso, como se trata de relação de consumo, impõe-se a aplicação da possibilidade de inversão do ônus da prova.

Além disto, outra dificuldade é a alteração da política de *cookies* atualmetne praticada pelos principais sites, dentre eles o Portal que será analisado mais a frente, porém com a entrada em vigor da Lei 12.965, de 23 de Abril de 2014 (Marco Civil da Internet):

> [...] de acordo com o artigo 7º inciso VI do atual texto, essa política deverá ser mudada [...] É importante destacar que as regras estabelecidas pelo projeto de lei nº 2.126/11 é dirigida para todos os usuários da rede, não importando em que lado ele se encontra ou sua natureza jurídica, seja esta particular e pública (SILVA, 2014, p. 12) .

Contudo o antigo Projeto de Lei nº 4.060 de 2012 não previa especificamente a forma e condições deste consentimento, o que sem dúvida é uma falha grave, visto que um dos princípios mais essenciais para que se garanta efetivamente a autodeterminação informativa é o princípio da necessidade de consentimento livre, expresso e informado[115]. Espera-se que tal omissão seja resolvida no novo processo de elaboração da legislação que ora se inicia com a consulta pública, pois atualmente a autodeterminação informativa só consta no texto do Marco Civil da Internet, que expressamente refere à forma e condições deste consentimento, que também devem ser aplicáveis à vedação do inciso VII.

Assim como as legislações uruguaia e argentina, o Marco Civil trouxe uma previsão de conteúdo do referido consentimento para que possa ser caracterizado como um consentimento efetivamente informado.

---

[114] Poderia ser propugnada uma analogia com o Código de Defesa do Consumidor (Lei nº 8.078 de 1990), e aos deveres de informação lá constantes, porém nestas situações a relação ficaria limitada ao reconhecimento da relação de consumo entre o detentor dos dados e o seu titular.

[115] E isso exige uma previsão clara e precisa sobre a necessidade e o conteúdo do consentimento mínimo que se exige do titular para ter a possibilidade lícita de manejar os seus dados.

O art. 7º inciso VIII prevê ser direito do usuário da Internet obter

> [...] informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet. (BRASIL, 2014-a).

Portanto claramente a legislação brasileira avançou ao limitar a utilização dos dados pessoais a finalidades que cumpram uma série de requisitos, dentre eles a justificativa da sua coleta, bem como a necessidade de previsão de sua explicitação nos contratos de prestação de serviço e termos de uso, que são exemplos de previsões legais que garantem uma efetiva autodeterminação informativa.

Como esclarece Paulo Molon (2009, p. 38):

> Ademais, tem se tornado prática usual na Internet a coleta de dados pessoais, outorgando aos provedores de tais serviços o gerenciamento de um conjunto significativo de dados sobre os usuários. Na ausência de uma lei de proteção de dados pessoais no ordenamento jurídico nacional, capaz de garantir ao cidadão a adequada tutela de tais informações, faz-se necessário antecipar no Marco Civil da Internet algumas regras relativas ao registro e tratamento de tais dados.

Isto ocorre porque somente ao se vincular a finalidade àquela prevista no momento da coleta do dado pessoal, bem como defini-la em um documento expresso e escrito fornecido ao titular, é que este usuário estará efetivamente cedendo, de forma consentida e informada, o seu dado pessoal.

Desta forma, Jesus e Milagre (2014, p. 19):

> Em síntese, com o Marco Civil o usuário tem o controle de seus dados e será informado nos contratos, de forma destacada, sobre como serão protegidos os dados fornecidos espontaneamente ou coletados automaticamente. Mais: terá a garantia de que somente os dados necessários serão coletados e especificamente para a finalidade destinada. Por exemplo, o usuário que fornece dados para ingressar em uma rede social não o fez para receber mensagens publicitárias ou marketing direcionado.

A autodeterminação informativa efetiva está prevista pelo Marco Civil da Internet quando prevê, no art. 7º inciso IV, que o usuário tem direito ao "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais." (BRASIL, 2014-a).

Apesar desta previsão clara de que deve ser garantido ao titular dos dados o direito de consentir com a sua utilização, a sua mera definição não concede efetivamente ao usuário a autonomia que seria desejável.

Mesmo que o usuário consinta expressamente com determinado tratamento de seus dados pessoais, não há no Marco Civil qualquer previsão que lhe garanta o direito ao acesso, instrumento por meio do qual pode efetivamente controlar o uso e o tratamento a que seus dados estão submetidos e verificar se correspondem aos consentidos.

O Projeto de Lei nº 4.060 de 2012 previa, em seu artigo 19, que o titular poderia em "qualquer momento, requerer o bloqueio do tratamento de seus dados pessoais, salvo se a manutenção do tratamento for necessária à execução de obrigações legais ou contratuais."(BRASIL, 2014-b). Porém esta medida era insuficiente, pois o mero bloqueio não garantiria o acesso efetivo aos dados pessoais registrados, visto que a autodeterminação informativa exige que o titular possa ter uma atuação consciente e capaz de compreender qual o tratamento que ele consentiu e de entender precisamente em que momento aquele seu dado foi submetido a tratamento diverso.

A única previsão que a legislação infraconstitucional traz referente ao direito ao acesso é aquela pertinente à Lei nº 9.507, de 12 de novembro de 1997, que, segundo sua ementa, "Regula o direito de acesso a informações e disciplina o rito processual do habeas data." (BRASIL, 2014-c).

Sabendo-se foi muito anterior a qualquer previsão legal pertinente à utilização da Internet no Brasil, a Lei nº 9.507, de 12 de novembro de 1997 (Lei do *Habeas Data*) deverá ser analisada sob a ótica de ser o instrumento que possibilita ao titular acessar suas informações pessoais, localizados em ambientes virtuais.

Conforme o art. 2º da Lei nº 9.507 de 1997: "O requerimento será apresentado ao órgão ou entidade depositária do registro ou banco de dados e será deferido ou indeferido no prazo de quarenta e oito horas." E o parágrafo único preleciona: "decisão será comunicada ao requerente em vinte e quatro horas."(BRASIL, 2014-c).

O prazo previsto para a resposta ao requerimento de acesso pela legislação brasileira, utilizando-se das previsões do *Habeas Data*[116], é o menor dos países analisados, porém a lei não estabalece as razões de recusa ao fornecimento. Além disto, não prevê consequências ao responsável pelo banco de dados que se recusa ilicitamente a fornecer tais dados.

[116] Neste caso o *Habeas Data* estaria sendo utilizado para bancos de dados privados, o que poderia causar problemas de aplicabilidade, especialmente considerando que este instrumento foi concebido para acesso a bancos de dados públicos e/ou de caráter público.

Outro grande problema é que este dever de conceder o acesso restringe-se ao órgão ou entidade depositária, porém não esclarece como garantir tal direito na situação onde os dados pessoais estão com outra entidade que funciona como uma mera usuária do banco de dados, o que demonstra a inadequação dessa legislação para responder aos inéditos problemas derivados do uso das tecnologias da informação e comunicação.

Estas dificuldades surgem pelo fato de que as previsões que visam instrumentalizar o direito ao acesso foram estabelecidas em momento muito anterior à realidade dos bancos de dados digitais, portanto aquelas previsões deveriam ser atualizadas e adapatadas a esta nova realidade.

Mais uma lacuna constante no Marco Civil e que não seria resolvida pelo texto agora arquivado projeto de Lei de Proteção de Dados refere-se ao direito do titular retificar informações a seu respeito que entende estarem equivocadas. Conforme prevê o art. 4º da lei do *Habeas Data*, "Constatada a inexatidão de qualquer dado a seu respeito, o interessado, em petição acompanhada de documentos comprobatórios, poderá requerer sua retificação."(BRASIL, 2014-c)

Nesta questão a legislação brasileira ficou muito aquém das previsões dos seus países vizinhos, visto que previu somente a possibilidade de retificação das inexatidões constantes nos bancos de dados, silenciando quanto à faculdade de atualização, supressão ou mesmo, como o fez a legislação argentina, de atribuição de confidencialidade.

Estas outras possibilidades envolvendo os bancos de dados são previsões que priorizam a autodeterminação informativa, pois concedem ao titular dos dados pessoais um grau mais elevado de controle sobre as suas informações pessoais, estejam em bancos de dado públicos ou privados.

Quanto à ação específica para proteção de dados pessoais pelas previsões da legislação brasileira, resta ao titular a utilização do *Habeas Data*, porém tal garantia constitucional foi pensada para o controle de dados em arquivos físicos e de caráter público[117], condições que podem servir como obstáculos ao efetivo exercício da autodeterminação informativa.

Por ter sido regulamentado para arquivos físicos, a legislação do *Habeas Data* não teve qualquer dificuldade ao estabelecer como sujeito passivo apenas o responsável pelo banco de dados, visto que o acesso a estas informações por terceiros ocorreria em situações extremamente excepcionais. Porém os arquivos digitais são tecnicamente de amplo e irrestrito

[117] Os tribunais superiores têm entendimentos sistemáticos limitando a utilização deste instrumento, a exemplo do Supremo Tribunal Federal no Recurso Extraordinário, com Repercusão Geral reconhecida nº 673.707-MG (BRASIL, 2015) e no Superior Tribunal de Justiça com o Recurso Especial nº 1.411.585- PE (BRASIL, 2015-A).

acesso, portanto podem ser direcionados a diversos usuários que não o responsável por estes dados, que, por sua vez, podem utilizar-se deles de forma indiscriminada, dificultando o controle do titular.

No mesmo sentido, por limitar-se a arquivos de caráter público, Constituição Federal de 1988 e a legislação do *Habeas Data* acaba por condicionar o efetivo direito ao acesso, o que cria um óbice ao seu exercício, pois determinadas informações pessoais podem ser compreendidas como não tendo caráter público, mas, em conjunto com outras ou isoladamente em determinadas condições, podem ser prejudiciais ao titular.

Por fim, outra grande falha da legislação brasileira é a ausência de regulamentação para a criação de um órgão específico de controle de dados pessoais com competência e atribuições semelhantes àqueles criados na legislação uruguaia e na legislação argentina. A existência de um órgão com competência específica nesta matéria é essencial, pois permite um controle das relações jurídicas entre usuários de arquivos e titulares destas informações, e que, ao mesmo tempo não impede o exercício das atividades daqueles, protege os direitos destes.

2.2.4 Os contrastes legislativos: possibilidades e desafios à hamonização da proteção de dados pessoais nos estados analisados.

Com base nas três legislações até o momento investigadas, verifica-se que o nível de proteção é muito semelhante na Argentina e no Uruguai, e menos protetivo no Brasil. Tal situação não deveria ocorrer, considerando que este Estado foi o último a legislar sobre o uso da *Internet* e poderia coletar experiência de duas décadas de regulamentação da utilização dos dados pessoais nos seus países vizinhos.

A principal razão para este desnível entre os dois primeiros países e o terceiro deve-se ao fato de ele não ter especificamente regulamentado a matéria da proteção de dados pessoais, mantendo somente algumas previsões no Marco Civil da Internet, e outras na lei do *Habeas Data*.

Tal desnível de proteção reflete-se nos critérios escolhidos para a análise, sendo eles: a) conceituação de dados pessoais e sua classificação/suas espécies; b) regulamentação do uso do dado sensível; c) consentimento do usuário para captação e uso dos dados de acordo com a finalidade prevista; d) veracidade dos dados pessoais registrados; e) procedimentos para acesso e retificação de dados; f) existência e funçõe do órgão de controle.

Quando da primeira categoria conceitual que tratou das definições que as legislações apresentam para os termos “dados pessoais” e “dados sensíveis”, verifica-se que tanto Argentina como Uruguai utilizaram definições semelhantes, sendo que elas apresentaram um aspecto negativo pelo fato de não referirem a principal característica do dado sensível, isto é, potencialidade de causar discriminação do titular, denotando-se, portanto, que o rol de dados considerados sensíveis poderiam ser taxativos e não meramente exemplificativos.

Por outro lado, ambas tiveram o aspecto positivo de estenderem a definição de dados pessoais àqueles que potencialmente possam identificar determinado indíviduo, quando estabelecem que dado pessoal sera aquele referente à pessoa determinada ou determinável.

Já a legislação do Brasil claramente, quando das definições, apresentou um nível aquém dos demais países, pois, além de também restrigir o conceito de dado pessoal sensível com o Projeto de Lei de Proteção de Dados Pessoais, pretendia restrigir excessivamente o próprio conceito de dado pessoal, ao afirmar que seria aquele precisa e exatamente referente a uma pessoa determinada.

No que pertine à segunda categoria que se preocupa com tratamento concedido aos dados pessoais sensíveis como forma de verificar se as legislações distinguem corretamente os dados segundo a possibilidade de violação da personalidade do usuário, Argentina e Uruguai possuem legislações cujas regras são protetivas, pois vedam, em regra geral, o tratamento de dados pessoais sensíveis, porém a grande dificuldade surge das exceções a esta regra, sobretudo considerando o alto grau de amplitude conceitual destas.

No caso, a legislação argentina prevê exceções um pouco mais restritas, podendo ser avaliada como tendo um grau de protetividade maior em favor do internauta, pois autoriza o tratametno destes dados no caso de intereses geral, previsto em lei. Por outro lado, a legislação uruguaia autoriza este tratamento quando a autoridade pública tiver um mandato legal para fazê-lo, mesmo no caso da ausência de caracterização legal deste dado como sensível.

No mesmo sentido, a legislação brasileira, pelo projeto de lei que pretendia regulamentar a matéria, também traria como regra a vedação do tratamento de dados sensíveis, porém teria como exceção a exigência de imposição legal, o que a aproximaria mais das previsões da legislação da Argetina do que da legislação do Uruguai.

Quanto à exigência de consentimento do usuário para o tratamento dos seus dados pessoais, bem como quanto à utilização de dados pessoais, as três legislações, de alguma forma, tratam da matéria. A legislação argentina trouxe esta previsão, regulamentando inclusive as características da informação, que devem ser prestadas ao titular quando do

recolhimento dos seus dados. Na esteira destas previsões, também vinculou a utilização do dado pessoal à finalidade informada ao usuário no momento da captação das informações pessoais.

De forma semelhante, a legislação uruguaia contemplou tanto a necessidade de consentimento expresso e informado do titular, quando a vinculação do tratamento dos dados pessoais à finalidade da captação como princípios do seu tratamento.

A legislação brasileira conta atualmente com a previsão do § 3º do art. 9º do Marco Civil da Internet, que impede que o tratamento de dados pessoais ou a sua cessão a terceiros pelo responsável por bancos de dados pessoais ocorra sem o prévio e expresso consentimento do usuário titular destes dados.

O quarto critério de análise refere-se à qualidade/veracidade do dado pessoal registrado, onde se buscou constatar se as legislações preocuparam-se com a legitimidade daquelas informações vinculadas a determinado indivíduo.

As legislações do Uruguai e da Argentina, comparativamente investigadas, contemplam a questão da qualidade dos dados pessoais recolhidos em bancos, registros ou arquivos, referindo que devem ser verdadeiros, corretos, precisos e vinculados à finalidade expressa ao titular quando de sua captação. Por outro lado, a legislação brasileira não conta com previsões semelhantes no Marco Civil da Internet, tampouco havia uma previsão expressa no projeto de lei que pretendia regulamentar especificamente a proteção de dados pessoais.

A quinta característica que serviu como parâmetro para a análise comparativa foi se estas legislações concedem ao titular as possibilidades de acesso, retificação, supressão e demais direitos a eles pertinentes, questões essenciais para viabilizar que este usuário possa controlar a utilização e eventualmente motivar retificação do conteúdo de tais informações.

Neste aspecto, a legislação argentina mostrou-se menos retritiva ao exercício destes direitos que a legislação uruguaia, exigindo que o titular apenas prove a sua identidade e, no caso da titularidade dos sucessores, garantiu a eles incondicionalmente o exercício destas prerrogativas em face dos dados do titular. Já a legislação uruguaia exigiu que os sucessores fossem declarados com tal condição pelo juiz da partilha, algo que dificulta o exercício de tais prerrogativas.

Dentre as legislações dos países analisados aquele que por ora apresenta o menor grau de proteção aos internautas é o Brasil, pois ele ainda não tem uma legislação específica regulamentando o acesso aos dados pessoais digitais e tampouco havia menção, no Projeto de

Lei arquivado em 31 de janeiro, de normatizar o acesso dos sucessores, relegando as suas previsões à legislação que regulamenta a garantia constitucional do *Habeas Data*.

Devendo-se considerar que a Lei nº 9.507 de 1997 foi pensada para outro contexto e outra realidade histórica que não tem a possibilidade de comtemplar satisfatoriamente os dados pessoais arquivados em bancos de dados pessoais digitais.

E, por fim, a característica final que justificou a análise tratou da existência, atribuições e competências de um órgão de controle e de proteção de dados pessoais, autoridade administrativa que, dentre as suas finalidades exclusivas, deverá exigir dos gestores de bancos de dados o respeito às previsões das legislações em análise, bem como e principalmente proteger os titulares dos dados pessoais.

Neste ponto as legislações da Argentina e do Uruguai previram estes órgãos, concendendo a eles uma série de atribuições, tanto de caráter conciliatório entre os titulares dos dados pessoais e os usuários e responsáveis pelos bancos, arquivos ou registros, como de caráter sancionatório e punitivo, sendo que a legislação argentina inclusive concedeu ao seu órgão de controle competência para ações penais.

Por outro lado, tanto a legislação brasileira existente (Marco Civil da Internet e Lei do *Habeas Data*) quanto à experiência da proposta de regulamentação (Projeto de Lei de Proteção de Dados Pessoais, agora arquivado) não contemplam a criação de um órgão específico para tratar da matéria, o que sem dúvida é uma das maiores falhas do sistema de proteção brasileiro.

2.3 OS REFLEXOS DA LEGISLAÇÃO NA PRÁTICA DOS PROVEDORES DE ACESSO: DESAFIOS À PROTEÇÃO DE DADOS PESSOAIS EM FACE DA SEGMENTAÇÃO COMPORTAMENTAL.

No Brasil a implementação da *Internet* é regulamentada pelo Comitê gestor da *Internet* no Brasil (CGI.br)[118], um órgão criado pela Portaria Interministerial nº 147 entre o Ministério da Ciências e Tecnologia e o Ministério das Comunicações.

[118] Conforme previsto em seu site, destacam-se dentre suas atribuições e responsabilidade: "a proposição de normas e procedimentos relativos à regulamentação das atividades na Internet; a recomendação de padrões e

Tal comitê tem como uma das suas principais atribuições a coleta, a organização e a disseminação de informações sobre os serviços de *Internet*, incluindo indicadores e estatísticas.

Para exercer esta função, foi criado em 2005 o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br), vinculado ao Núcleo de Informação e Coordenação do Ponto BR (nic.br), uma entidade civil sem fins lucrativos que, desde dezembro de 2005, implementa as decisões e projetos do Comitê Gestor da *Internet* no Brasil.

Em 2011 o CETIC.br (2011, p. 15) realizou uma pesquisa focada nos provedores de acesso à *Internet* no Brasil, onde constatou que:

> A inclusão digital no Brasil depende fundamentalmente da infraestrutura física dos serviços de *Internet*. Os provedores de serviço de *Internet* (PSI) – instituições que se conectam à*Internet* por meio de um ou mais acessos dedicados e tornam o acesso disponível a terceiros a partir de suas instalações – são os pilares de sustentação do sistema, por deixarem a rede mundial de computadores ao alcance dos cidadãos. Pode-se inferir que o acesso está diretamente relacionado aos serviços oferecidos pelos PSI. [...] A contribuição maior dessa pesquisa é mapear os provedores de serviços de acesso.

Tal pesquisa verificou que, apesar de existirem 1.934 provedores de *Internet* no Brasil, 78% (setenta e oito por cento) das conexões dos brasileiros com a *Internet* (CETIC.BR, 2011, p. 28) é feito por apenas 06 (seis) provedores pertencentes a um número pequeno de empresas. Estes provedores são considerados provedores de grande porte, pois contam com mais de 900 (novecentos) mil clientes.

A pesquisa não afirma textualmente, porém, conforme noticiado pelo Clipping do Núcleo de Informação e de Coordenação do Ponto BR, as maiores empresas neste setor são a Net (Virtual), a GVT, a OI (Virtua), a Embratel (Giro), a CTBC Telecom e a Telefônica, proprietária do provedor de acesso "Terra" (DE LUCA, 2013).

Considerando a análise do subcapítulo anterior e tendo em conta que destes seis provedores apenas o "Terra", de propriedade da Telefônica, atua nos países que tiveram as suas leis de proteção de dados analisadas, este provedor será o objeto do presente subcapítulo.

Porém tal análise não poderá ocorrer diretamente sobre a forma como o provedor de acesso trata os dados pessoais dos seus usuários, e por isso optou-se por pela análise do seu

---

procedimentos técnicos operacionais para a Internet no Brasil; o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil; a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país; a coordenação da atribuição de endereços Internet (IPs) e do registro de nomes de domínios usando <.br>; a coleta, organização e disseminação de informações sobre os serviços Internet, incluindo indicadores e estatísticas." (CGI.br, 2014)

Termo de Política de Privacidade, considerado a manifestação mais clara de qual a forma de tratamento a que serão submetidos os dados pessoais dos internautas.

Como forma de gerar uma comparação objetiva, preferiu-se eleger os termos de uma empresa específica que estivesse dentre as maiores e cujos serviços fossem de utilização massiva nestas nações. Portanto houve a escolha pelo Provedor de Acesso vinculado ao portal "Terra".

Não haveria como realizar uma efetiva comparação diante de termos produzidos por diferentes entes, visto que, como empresas multinacionais autônomas, as previsões de uma delas não necessariamente devem ser reproduzidas pelas demais. Consequentemente, as influências da legislação de cada país sobre os documentos emanados não seriam identificáveis.

Desta forma, a partir dos Termos de Políticas de Privacidade do portal "Terra", que mantém diretamente ou está vinculado a provedores de acesso nos países analisados, é possível verificar o tratamento que é destinado aos dados pessoais dos internautas, dados que são obtidos a partir de sua navegação na *Internet*.

2.3.1 "Política de Privacidad" acessível no Portal Terra da Argentina e do Uruguai.

Em um primeiro momento, é preciso esclarecer que o Termo de Política de Privacidade constante do portal "Terra" na Argentina, bem como dos demais serviços a ele vinculados, é o mesmo termo utilizado no Uruguai, pois inclusive não há a atuação do portal "Terra" com o domínio correspondente ao Uruguai.

O referido documento (TERRA ARGENTINA, 2014), denominado *Política de Privacidad*, preceitua que:

> Mediante este aviso, Terra Networks Argentina, S.A (en adelante TERRA) informa a los usuarios de los distintos portales de Internet de su propiedad (en adelante, los "Usuarios" y el "Portal") acerca de su política de protección de datos de carácter personal (en adelante, "los Datos Personales") para que los Usuarios determinen libre y voluntariamente si desean facilitar a TERRA los Datos Personales que se les puedan requerir o que se puedan obtener de los Usuarios con ocasión de la suscripción o alta en algunos de los servicios ofrecidos por TERRA en el Portal o a través del Portal. TERRA se reserva el derecho a modificar la presente política para adaptarla a novedades legislativas o jurisprudenciales así como a prácticas de la industria. En dichos supuestos, TERRA anunciará en esta página los cambios introducidos con razonable antelación a su puesta en práctica[119].

[119]Tradução do pesquisador: "Mediante este aviso, Terra Networks Argentina, SA (TERRA) informa aos usuários de vários portais de *Internet* de sua propriedade (doravante denominados "Usuários" e "*Website*") sobre a sua política de proteção de dados pessoais (doravante "dados Pessoais") para que os usuários determinem livre

O documento analisado irá obrigar qualquer serviço oferecido pelos *sites* vinculados ao portal "Terra", dentre os quais o de provedor de acesso à Internet. Além disso, este trecho prevê que o usuário deverá livre e voluntariamente consentir com a disposição dos seus dados pessoais, porém não cientifica que esta autorização também deverá ser informada.

Esta omissão é relevante no sentido de que apenas quando ao usuário é garantida a possibilidade de consentir de forma informada, ou seja, tendo conhecimento do tratamento que será dado aos seus dados, é que será respeitada a sua autodeterminação informativa (PÉREZ LUÑO, 2005).

Este termo ainda esclarece que: "Ciertos servicios prestados en el Portal pueden contener condiciones particulares con previsiones específicas en materia de protección de Datos Personales.[120]" (TERRA ARGENTINA, 2014). Portanto os serviços de provedores de acesso vinculados ao "Terra" poderão disponibilizar documentos semelhantes a este termo, porém estes documentos não poderão claramente reduzir o grau de proteção do internauta.

A referência à existência de termos específicos para determinados serviços tem a sua relevância, pois é essencial compreender que, para cada ente que intervém no acesso do usuário à *Internet*, deve ser atribuído um grau diferente de proteção. Por exemplo, um provedor de acesso tem uma responsabilidade maior na proteção de dados do usuário do que um provedor de *backbone*, pois enquanto este possibilita a conexão entre sistemas, aquele vincula e relaciona usuários a rede.

Ainda, o referido documento prevê (TERRA ARGENTINA, 2014):

> Los Datos Personales serán objeto de tratamiento automatizado e incorporados a los correspondientes ficheros automatizados de datos de carácter personal de los que TERRA será titular y responsable (en adelante, el "Fichero"). Con este objeto, TERRA le proporciona a los Usuarios los recursos técnicos adecuados para que, con carácter previo, puedan acceder a este aviso sobre la Política de Privacidad o a cualquier otra información relevante y puedan prestar su consentimiento a fin de que TERRA proceda al tratamiento automatizado de sus Datos Personales. Salvo en los campos en que se indique lo contrario, las respuestas a las preguntas sobre Datos Personales son voluntarias, sin que la falta de contestación implique una merma en la calidad o cantidad de los servicios correspondientes, a menos que se indique otra cosa[121].

---

e voluntariamente se desejam fornecer dados pessoais ao TERRA que possam ser obtidos com os usuários para assinatura ou registro para quaisquer serviços oferecidos por TERRA no Portal ou através dele. O TERRA se reserva o direito de alterar esta política para se adaptar à nova legislação ou jurisprudência, bem como as práticas da indústria. Nesses casos, TERRA anunciará nesta página as mudanças com antecedência razoável antes da implementação."

[120]Tradução do pesquisador: "Alguns serviços oferecidos no *site* podem conter condições com disposições específicas sobre a proteção de dados pessoais."

[121] Tradução do pesqusiador: "Os dados pessoais serão processados automaticamente e incorporados nos arquivos relevantes de dados pessoais (doravante denominado "Arquivo"), dos quais será o dono e responsável TERRA. Para este efeito, TERRA oferece ao usuário os recursos técnicos adequados para que antes pode acessar

Verifica-se que as disposições da legislação argentina influenciaram o referido documento em dois pontos. O primeiro refere-se à exigência de consentimento informado, quando o termo previamente possibilita ao internauta o acesso a ele, compreendendo qual a política a que ficarão submetidos os seus dados. Um segundo ponto refere-se propriamente às dimensões deste direito de informação, quando afirma que o usuário terá direito de entender se os questionamentos são voluntários ou obrigatórios, sendo que, no caso, os sistemas vinculados ao "Terra" preferem obter informações dos usuários de forma voluntária.

A terceira previsão claramente protetiva do referido documento afirma que o usuário não poderá sofrer perda na qualidade do serviço caso voluntariamente opte por não ceder seus dados pessoais, assim o termo privilegia o controle das informações pessoais pelo titular (RODOTÀ, 2008), uma autodeterminação informativa.

Em continuidade, quanto à qualidade dos dados pessoais, o documento refere:

> El usuario garantiza que los Datos Personales facilitados a TERRA son veraces y se hace responsable de comunicar a ésta cualquier modificación en los mismos. La recogida y tratamiento automatizado de los Datos Personales tiene como finalidad el mantenimiento de la relación contractual en su caso establecida con TERRA, la gestión, administración, prestación, ampliación y mejora de los servicios en los que el Usuario decida suscribirse, darse de alta o utilizar la adecuación de dichos servicios a las preferencias y gustos de los Usuarios, el estudio de la utilización de los servicios por parte de los Usuarios, el diseño de nuevos servicios relacionados con dichos servicios, el envío de actualizaciones de los servicios, el envío, por medios tradicionales y electrónicos, de información técnica, operativa y comercial acerca de productos y servicios ofrecidos por TERRA y por terceros actualmente y en el futuro. La finalidad de la recogida y tratamiento automatizado de los Datos Personales incluye igualmente el envío de formularios de encuestas, que el Usuario no queda obligado a contestar[122] (TERRA ARGENTINA, 2014).

Verifica-se que há uma influência da exigência de qualidade dos dados pessoais, o que privilegia o princípio da veracidade previsto nas legislações do Uruguai e da Argentina, porém esta exigência de qualidade é repassada exclusivamente ao internauta, sendo que a legislação desses países exige de todos os polos da relação de recolhimento e tratamento dos

---

este aviso sobre a Política de Privacidade ou qualquer outra informação relevante e dar o seu consentimento para TERRA realizar o processamento automático seus dados pessoais. Exceto nas áreas onde indicado o contrário, as respostas às perguntas sobre dados pessoais são voluntárias, sem a falta de resposta implica uma diminuição da qualidade ou quantidade dos serviços, salvo indicação em contrário".

[122] Tradução do pesquisador: "O usuário garante que os dados pessoais fornecidos ao TERRA são verdadeiros e é responsável por comunicar qualquer alteração nos mesmos. A recolha e tratamento de dados pessoais visa a manutenção da relação contratual estabelecida com TERRA, gestão, administração, prestação, ampliação e melhoria dos serviços em que o usuário decide se inscrever, registrar ou usar a adequação desses serviços às preferências e gostos dos usuários, o estudo da utilização dos serviços pelos usuários, o desenho de novos serviços relacionados a estes serviços, o envio de atualizações de serviço, transporte, por meios tradicionais e eletrônicos, de informações técnicas, operacionais e comerciais sobre produtos e serviços oferecidos por terceiros TERRA e agora e no futuro. A finalidade da recolha e tratamento de dados pessoais também inclui o envio de formulários de pesquisas, que o usuário não é obrigado a responder"

dados este respeito. Para tanto, o termo deveria ter estabelecido que usuário e os serviços vinculados ao “Terra” se comprometem com a veracidade dos dados arquivados, pois a exigência de qualidade dos dados não se constitui em uma obrigação exclusiva do titular de tais informações.

Após, nesta previsão consta que o recolhimento e o tratamento dos dados pessoais funcionarão para algumas finalidades, a grande maioria vinculada à correta e adequada prestação dos serviços pelos entes vinculados ao portal “Terra”, porém alguns são preocupantes. Destaca-se a questão do desenvolvimento e oferta de novos serviços relacionados a estes. Esta previsão acaba por se configurar em uma forma de burlar os princípios da finalidade e do prévio consentimento, pois os dados pessoais do usuário são cedidos para um determinado e específico serviço, e não para possibilitar o desenvolvimento de outros.

Os novos serviços que eventualmente venham a ser desenvolvidos não podem partir da utilização dos dados pessoais dos usuários, sem que estes tenham a oportunidade de consentir com tal utilização, caso contrário, a autodeterminação informativa deste indíviduo estará sendo violada, e, portanto, o consentimento deveria ser individualizado para cada serviço.

Outra previsão preocupante é aquela que se refere à possibilidade de utilização dos dados pessoais dos usuários para oferta de serviços disponibilizados pelos entes vinculados ao “Terra” ou por terceiros. Tal previsão esvasia completamente a eficácia de diversas previsões estabelecidas na legislação argentina, bem como enfraquece os princípios elencados pela legislação uruguaia.

Não há como garantir que os dados serão tratados exclusivamente para a finalidade a qual foram captados, nem mesmo quando os sujeitos que determinam estas finalidades irão utilizar estes dados. O termo não garante um mínimo de proteção de dados pessoais dos usuários quando as finalidades elencadas possibilitam a sua utilização por terceiros.

A eficácia das regras de proteção aos dados pessoais dos internautas pressupõe um respeito aos polos da relação jurídica que se estabelece entre quem é o titular de tais informações e quem se responsabiliza por tratá-las. Assim, se estes polos são flexibilizados, autorizando terceiros a ter acesso a estes dados, estas regras não são mais capazes de garantir um mínimo de proteção aos usuários, pois estes terceiros não participam do principal ato jurídico que torna esta utilização de dados pessoais lícita, o consentimento prévio e informado do titular.

Quanto aos níveis de segurança e proteção, o Termo de Política de Privacidade expressamente prevê:

> TERRA ha adoptado los niveles de seguridad de protección de los Datos Personales legalmente requeridos, y procura instalar aquellos otros medios y medidas técnicas adicionales a su alcance para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los Datos Personales facilitados a TERRA. En particular, TERRA utiliza sistemas de seguridad SSL (Secure Socket Layer) que, a través de sistemas de certificados y cifrado, permiten comprobar la autenticidad del Portal Terra desde donde se recaban sus Datos Personales, así como la integridad y confidencialidad de sus Datos Personales durante la transmisión de sus Datos Personales (Ud. Puede comprobar la implementación del SSL al registrarse dado que la página de registro comienza con "htpps", en lugar del "http" de entornos no seguros, y le aparecerá un pequeño candado cerrado en la parte inferior de su navegador). Ello no obstante, el Usuario debe ser consciente de que las medidas de seguridad en Internet no son inexpugnables[123] (TERRA ARGENTINA, 2014):.

Estas previsões são reflexos dos deveres de segurança e integridade dos sistemas informatizados que tratam de dados pessoais. O responsável pelo tratamento de dados pessoais deve tecnicamente tomar todas as medidas pertinentes à proteção do seu sistema, pois ele contém informações que não lhe pertencem, mas que recebeu a autorização de uso do titular, para finalidades específicas.

O termo orienta o usuário a contribuir com estas medidas técnicas, visualizando, por exemplo, no seu navegador se o *site* que está acessando é realmente vinculado ao "Terra" antes de prestar qualquer informação que esteja sendo solicitada. Porém todo o sistema informatizado corre o risco de sofrer ataques e invasões. Em decorrência desta realidade, o próprio termo alerta que o titular deve estar consciente de que na Internet não há sistema informatizado completamente inexpugnável.

Quanto à possibilidade de cessão de dados o termo refere que:

> TERRA podrá ceder, en su caso, los Datos Personales a las sociedades del Grupo TELEFONICA con las mismas finalidades que se han indicado para la recogida de los Datos Personales por parte de TERRA en relación con sus respectivos productos y servicios. A los efectos de esta Política de Privacidad, se consideran sociedades del Grupo TELEFONICA aquellas sociedades en las que TERRA o la sociedad matriz de dicho grupo, Telefonica S.A, directa o indirectamente [...] En ciertos casos, además, se propone ceder los Datos Personales a terceros. Cuando proceda, esta circunstancia será debidamente advertida a los Usuarios en los formularios de recogida de Datos Personales, junto con la identificación de la sociedad que los ceda y dicho tercero, el tipo de actividades a las que se dedica y la finalidad a que responde la cesión. El Usuario podrá oponerse en

[123]Tradução do pesquisador: "TERRA adotou os níveis de proteção de dados pessoais legalmente exigido de segurança e instala todos os meios e medidas técnicas ao seu alcance para evitar a perda, mau uso, alteração, acesso não autorizado e roubo dos dados pessoais fornecidos ao TERRA. Em particular, TERRA usa (Secure Socket Layer) sistemas de segurança SSL através de certificados e sistemas de criptografia que permite examinar a autenticidade do Portal Terra, a partir do qual as informações pessoais são coletadas, bem como a integridade e confidencialidade dos seus dados pessoais durante a transmissão dos seus dados pessoais (Ud. pode verificar a implementação de SSL para registrar porque a página de inscrição começa com "https" em vez de "http" ambientes inseguros, e um pequeno cadeado fechado aparecerá na inferior do seu navegador). Não obstante, o usuário deve estar ciente de que as medidas de segurança na Internet não são inexpugnáveis."

> todo momento a cualquiera o todas las cesiones precitadas mediante el ejercicio de sus derechos según se detalla más abajo[124] (TERRA ARGENTINA, 2014): .

Portanto o termo autoriza a cessão de dados pessoais a empresas pertencentes ao mesmo grupo econômico do "Terra", a Telefônica S.A, porém vincula esta utilização àquelas finalidades constantes no presente termo.

Esta previsão traz um caráter positivo, pois estende a estas empresas todas as obrigações constantes no termo, tornando-as também responsáveis pelo cumprimento das finalidades expressas quando da captação dos dados pessoais, o que estende um mínimo de proteção a todo e qualquer tratamento que tais informações venham a submeter.

Porém esta previsão, assim como a possibilidade de utilização dos dados para ofertas de serviços de terceiros, também enfraquece o sistema de proteção, pois amplia excessivamente um dos polos vinculados pelo termo de consentimento livre e informado fornecido pelo titular dos dados.

Quanto os direitos de acesso, cancelamento, retificação ou oposição, o Termo refere que:

> Los Usuarios tienen reconocidos y podrán ejercitar los derechos de acceso, cancelación, rectificación y oposición, así como tienen reconocido el derecho a ser informados de las cesiones realizadas contactando con TERRA a través del correo electrónico http://www.terra.com.ar/mensajes/app/formulario[125].

Esta previsão é um reflexo claro da legislação argentina, pois garante expressamente o direito ao acesso e os seus consectários – retificação, atualização, supressão. Por outro lado, o termo erra ao vincular um meio específico para o exercício destes direitos quando a própria legislação daquele país estabelece que o acesso deve ser concedido ao titular através do meio que ele escolher, e não através da forma estabelecida unilateralmente pelo Termo de Política de Privacidade.

---

[124]Tradução do pesquisador: "TERRA poderá ceder, se for o caso, os dados pessoais a empresas do Grupo Telefónica com os mesmos fins que os indicados para a coleta de dados pessoais do TERRA em relação aos seus produtos e serviços. Para os efeitos desta Política de Privacidade, são consideradas empresas do grupo TELEFONICA as empresas em que a empresa-mãe TERRA ou aquele grupo, Telefônica SA, direta ou indiretamente [...] Em alguns casos, além disso, propõe-se a transferência de dados pessoais a terceiros. Se for o caso, isto será devidamente informado aos usuários nas formas de recolha de dados pessoais, juntamente com a identificação da empresa atribuir e tal terceiro, o tipo de atividades que realiza e o propósito por trás da atribuição. Os usuários podem opor-se a qualquer momento para qualquer ou todas as atribuições acima mencionadas, através do exercício de seus direitos, conforme detalhado abaixo"

[125]Tradução do pesquisador: "Usuários reconhecem e poderão exercer os seus direitos de acesso, cancelamento, retificação e oposição, e também têm o direito de serem informados sobre as transferências feitas contatando TERRA via e-mail http://www.terra.com.ar / posts / app / form"

Ainda, o termo omite-se quanto à possibilidade do titular atribuir a confidencialidade a determinadas informações pessoais, direito que a ele é expressamente garantido pela lei argentina de proteção de dados pessoais. Essa atribuição de confidencialidade é o direito, decorrente do acesso aos dados pessoais próprios, que melhor privilegia a autodeterminação informativa (PÈREZ-LUÑO, 2005), pois permite ao titular de dados pessoais a classificação das suas informações, de forma a determinar os níveis de proteção que pretende que elas recebam.

Por fim, o documento refere que o "Terra" poderá utilizar-se de *cookies*, estabelecendo que:

> TERRA puede utilizar cookies cuando un Usuario navega por los sitios y páginas web del Portal. Las cookies que se pueden utilizar en los sitios y páginas web del Portal se asocian únicamente con el navegador de un ordenador determinado (Usuario anónimo), y no proporcionan por sí el nombre y apellidos del Usuario. Gracias a las cookies, resulta posible que TERRA reconozca a los navegadores de los Usuarios registrados después de que éstos se hayan registrado por primera vez, sin que se tengan que registrarse en cada visita para acceder a las áreas y servicios reservados exclusivamente a ellos. Las cookies de TERRA no pueden leer datos de los archivos cookie creados por otros proveedores. TERRA cifra los datos identificativos del Usuario para mayor seguridad. El Usuario tiene la posibilidad de configurar su navegador para ser avisado en pantalla de la recepción de cookies y para impedir la instalación de cookies en su disco duro. Por favor, consulte las instrucciones y manuales de su navegador para ampliar ésta información. Para utilizar el Portal, no resulta necesario que el Usuario permita la instalación de las cookies enviadas por TERRA, sin perjuicio de que en tal caso será necesario que el Usuario se registre como usuario de cada uno de los servicios cuya prestación requiera el previo registro. Las cookies que se utilizan en los sitios y páginas web del Portal pueden ser servidas por TERRA, en cuyo caso se sirven desde los distintos servidores operados por éstas, o desde los servidores de determinados terceros que nos prestan servicios y sirven las cookies por cuenta de TERRA (como por ejemplo, las cookies que se emplean para servir la publicidad o determinados contenidos y que hacen que el Usuario visualice la publicidad o contenidos en el tiempo, número de veces y forma predeterminados). Siempre que no haya activado la opción que impide la instalación de cookies en su disco duro, Ud. puede explorar su disco duro siguiendo el manual de instrucciones y ayuda de sus sistema operativo (normalmente, en sistemas operativos Windows deberá consultar la carpeta "C (o la unidad de disco correspondiente)/Windows/Cookies" para conocer con mayor detalle cada servidor desde donde se envían las cookies[126].

[126]Tradução do pesquisador: "TERRA pode utilizar *cookies* quando um usuário navega sites e páginas do Portal na *web*. Os *cookies* que podem ser usados nos *sites* e páginas *web* do Portal associam-se unicamente com o navegador de um determinado computador (usuário anônimo) e não fornecem o nome completo do usuário. Graças aos *cookies*, é possível que TERRA reconheça os navegadores de usuários registrados depois de terem se registrado pela primeira vez, sem ter que se registrar a cada vez que acessar as áreas e serviços reservados exclusivamente para eles. Os *cookies* do TERRA não podem ler dados de arquivos *cookie* criados por outros provedores. TERRA criptografa os dados que identifiquem o usuário para maior segurança. Os usuários têm a possibilidade de configurar seu navegador para serem avisados quando receberem *cookies* e recusar o uso de *cookies* no seu disco rígido. Por favor, consulte as instruções e manuais do seu navegador para mais informações. Para utilizar o Portal, não é necessário que o usuário permita a instalação de *cookies* enviados por TERRA, apesar de que, nesses casos, exigirá que o usuário se registre como um usuário de cada um dos serviços que exigem inscrição prévia. Os *cookies* utilizados em *sites* e páginas *web* do Portal podem ser atendidas por TERRA, caso em que eles são dos distintos servidores operados por ele, ou a partir dos servidores de terceiros

A utilização dos *cookies* traz vantagens aos usuários, pois permite um acesso mais rápido a determinados *sites* a partir de um navegador específico em um computador determinado. Geralmente os sistemas que geram estes *cookies* não guardam diretamente relações de nomes e informações pessoais dos usuários, apenas a quantidade de acesso que aquele determinado terminal realizou em um determinado período de tempo.

Esta utilização, mesmo sendo considerada anônima, não deixa de potencialmente caracterizar-se como uma violação de dados pessoais, pois acaba relacionando interesses de determinado usuários – através de acesso por terminais habitualmente utilizados.

Os dados pessoais aqui não são direta e precisamente relacionáveis a um determinado indivíduo, mas podem, através de múltiplos cruzamentos de informações, revelar a sua identificação. Sendo assim, a utilização de *cookies* é um instrumento extremamente eficaz para a segmentação de comportamentos, considerando que habitualmente os indivíduos utilizam-se dos mesmos terminais para acessar a rede.

Desta forma, o termo de privacidade do "Terra" da Argentina apresentou-se como protetivo ao prever que a utilização desta ferramente técnica será feita, mas que ao usuário é garantido o direito de vedá-la ao alterar as configurações do seu navegador,.

Além disto, o termo demonstrou que respeita a autodeterminação dos usuários ao delegar a eles a possibilidade de bloquear o registro de *cookies* em seus discos rígidos, porém alertou que, caso utilizassem desta prerrogativa, deveriam se cadastrar em cada acesso aos serviços que exigem este tipo de procedimento.

Verifica-se que o Termo de Política de Privacidade no portal "Terra" na Argentina reflete muitas previsões da sua legislação, garantido o consentimento prévio livre e informado do usuário no momento da captação dos seus dados e vinculando a utilização destes dados pessoais à finalidade expressa no momento desta captação, além de garantir a ele direito ao acesso, retificação, dentre outros.

Porém, em alguns aspectos o termo poderia ser aprimorado, sobretudo quando se refereà possibilidade de utilização dos dados para envio de ofertas de serviços de terceiros, ou ainda quando vincula o direito ao acesso a um determinado meio específico.

---

que prestam serviços e servir os *cookies* em nome de TERRA (por exemplo, os *cookies* são usados para fins publicitários ou certos conteúdos e fazer o usuário visualizar a publicidade ou conteúdos em tempo, número de vezes por padrão). Sempre que você não tiver ativado a opção de impedir a instalação de *cookies* no seu disco rígido, você pode explorar seu disco rígido, seguindo as instruções e ajuda de seu sistema operacional (normalmente os sistemas operacionais Windows devem consultar o C (pasta "conduzir ou disco) / Windows / *cookies* "para obter mais detalhes sobre cada servidor a partir do qual os *cookies* são enviados."

2.3.2 As estratégias de informação sobre Dados Pessoais utilizadas pelo Provedor "Terra" Brasil

É preciso referir que o Termo de uso do Portal Terra, que se estende a todos os serviços oferecidos através deste portal, dentre os quais o de provedor de acesso à Internet, refere que:

> Este Termo regulamenta o uso do Portal TERRA, bem como os serviços/produtos neste oferecidos e fornecidos pelo TERRA NETWORKS BRASIL S.A., [...] aos usuários de Internet. A utilização do Portal por você implica na aceitação integral e plena deste Termo e Política de Privacidade. (TERRA BRASIL, 2014).

No referido termo (TERRA BRASIL, 2014), consta que:

> O TERRA preza pela segurança, sigilo e inviolabilidade de todos os dados cadastrais fornecidos por você. No entanto, você deve estar ciente que as medidas de segurança na Internet não são infalíveis, principalmente em razão da rápida evolução do ambiente virtual. Deste modo, o TERRA não se responsabiliza por danos e/ou prejuízos decorrentes de caso fortuito ou força maior. No mais, para que você saiba como o TERRA trata seus dados pessoais e protege a sua privacidade quando você acessa o Portal e os serviços neste disponibilizados, sugere-se a leitura da "Política de Privacidade do TERRA".

Portanto é essencial compreender que o Termo de uso remete a um segundo documento, responsável exclusivamente pela Política de Privacidade. Essa remissão tem um aspecto positivo, pois um documento específico tende a tratar com mais atenção as peculiaridades que o uso dos dados pessoais dos usuários exige. Porém esta remissão traz como aspecto negativo a dificuldade de acesso, pois ao contrário do Portal da Argentina, onde constavam os Termos de usos e a Política de Privacidade em um único documento, aqui o usuário deve buscar informações específicas em um segundo instrumento.

A dificuldade consiste no fato de que usualmente o internauta somente acessa, lê e consente com os documentos essencias para o que ele possa usufruir determinado serviço, não investigando ou se informando especificamente sobre outras temáticas dispostas em outros documentos[127]. Diante disso pode-se afirmar que haveria uma maior eficácia da política da empresa de houvesse um único documento que sintetizasse todas as questões pertinentes à política de uso dos serviços e de proteção de dados pessoais.

A análise, a partir deste momento, irá focar-se no referido documento denominado *Sua Privacidade é muito importante para o TERRA!*(TERRA BRASIL, 2014-a) que, ao contrário

[127] Desta forma o consentimento deste usuário ficaria prejudicado pela incompletude das informações imediatamente postas a sua disposição.

do Portal Argentino, caracteriza-se muito mais como uma série de orientações ao usuário do que propriamente como uma política efetiva de proteção de dados pessoais.

Inicialmente o aviso legal (TERRA BRASIL, 2014-a) prevê:

> Ao utilizar os serviços do TERRA, você compartilha inúmeras informações. Isso é muito importante para que os serviços sejam aprimorados e para que você tenha uma experiência online única e personalizada. Além disso, ao conhecer a política de privacidade do TERRA, você poderá contribuir para a modulação da sua experiência no Portal de acordo com as suas escolhas de navegação, tornando o TERRA cada vez mais seu. Para se adaptar às expectativas dos usuários, o TERRA poderá modificar a sua Política de Privacidade. Assim, é importante que você consulte nossa política regularmente e caso não concorde com as alterações promovidas, entre em contato com nossos canais de relacionamento ou descontinue o uso do seu serviço. Esta Política se aplica a todos os Serviços oferecidos e fornecidos pelo TERRA NETWORKS BRASIL S.A. com exceção daqueles que possuam Políticas de Privacidades específicas. A presente Política de Privacidade igualmente não se aplica a serviços e produtos oferecidos por empresas parceiras por meio de anúncios ou links no Portal TERRA.

Claramente o "Terra" admite a prática da segmentação comportamental, pois, logo no início do seu documento de proteção à privacidade, afirma que um dos seus grandes objetivos é prestar uma experiência personalizada, ou seja, adequada a cada usuário específico.Para que este usuário seja determinado, haverá uma análise dos seus dados pessoais, e ele será elencado a um nicho de indivÍduos ligados pelo seu comportamento.

Uma distinção do termo argentino é que, enquanto lá as possibilidades de alteração da Política de Privacidade ficam condicionadas à existência de modificações no tratamento concedido pela legislação ou de modificações de entendimentos jurisprudenciais. Porém as transformações no teor do termo no Brasil poderão ser feitas por mera conveniência e oportunidade do portal, para se adaptar, ou sob o pretexto de fazê-lo, às expectativas dos usuários, como ele mesmo afirma. Porém o termo não especifica como estas expectativas serão analisadas para basear tais alterações (se partirão de escolhas voluntárias e conscientes dos usuários, ou da análise dos seus dados de acesso e conexão).

Ainda, aqui ao contrário do afirmado no termo argentino, o documento excepciona de aplicabilidade os outros serviços que tenham termos específicos de proteção à privacidade, enquanto que lá ele determina que estes termos possam ter documentos específicos, mas que não necessariamente irão excepcióná-los da aplicabilidade do termo geral.

Em continuidade o documento (TERRA BRASIL, 2014-a) determina que "Listamos abaixo informações essenciais para uma navegação livre e consciente. Por favor, leia com atenção, pois estas disposições regulam a sua relação com o portal TERRA!" O início do termo já reflete a realidade jurídica de um país que não conta com uma legislação especifícia

de proteção de dados pessoais, pois não refere expressamente sobre a existência ou a eficácia de um nível legal mínimo de proteção de dados pessoais.

Ao afirmar que as previsões do termo irão regular a relação entre o usuário e o provedor de acesso à Internet, o documento reconhece que atualmente esta relação não conta com qualquer previsão legal específica que ampare os direitos fundamentais do cidadão internauta. O termo deveria ser adaptado após a publicação do Marco Civil da Internet, pois atualmente a proteção de dados pessoais passou a ter algumas previsões em normas infraconstitucionais que a amparam.

O referido documento (TERRA BRASIL, 2014-a) esclarece como o usuário irá compartilhar as informações com o "Terra", que acontecerá das seguintes formas:

> **Ao fornecer informações pessoais por meio de cadastros**. Ao criar uma conta própria para navegar no Portal, ao contratar os serviços neste disponibilizados, ao enviar formulários promocionais, ao postar conteúdos e em outras situações, você preenche cadastros, informando nome, endereço, CEP, número do registro junto ao Cadastro de Contribuintes (CPF), número do registro geral (RG), telefone para contato, nacionalidade, dados financeiros, que são armazenadas pelo TERRA. Assim, a veracidade dos dados fornecidos é de suma importância, tendo em vista ser por meio destes que o TERRA realizará qualquer contato com você, o que o torna responsável pelas declarações que prestar e que vierem a causar prejuízos a si mesmo, ao TERRA e/ou a terceiros.**Ao compartilhar informações de acesso durante a sua navegação**. Ao navegar no Portal TERRA sem desabilitar cookies

O aviso legal estabelece que o usuário possa fornecer suas informações pessoais ao "Terra" de duas formas distintas: através do preeenchimetno de cadastros, ou por intermédio da sua própria navegação.

Quanto à primeira hipótese, o que permite maiores comentários é o fato de o termo não trazer referência ao teor destes cadastros, ou seja, não estabelece se este fornecimento de informações será feito de forma informada pelo usuário. Haverá um efetivo exercício de autodeterminação informativa (PÈREZ-LUÑO, 2005), para além do exercício de uma mera autonomia privada, quando o usuário ao preencher tais documentos, for informado das finalidades para as quais os dados serão captados e tratados, para que o este possa posteriormente ter acesso a eles, caso estas previsões sejam desrespeitadas.

Outro ponto desta previsão refere-se ao fato de que o termo pretende elencar determinadas informações como pessoais, forma de atuação que torna ineficaz qualquer tentativa de proteção da personalidade e da privacidade, considerando que a grande maiora de informações pessoais que podem ser utilizadas não são diretamente fornecidas pelos usuários, mas sim decorrentes do cruzamento de dados pessoais (RODOTÀ, 2005, p. 35).

Já quanto à segunda hipótese – a utilização de *cookies* – para a navegação, o Termo (TERRA BRASIL, 2014-a) prevê que:

> Os cookies são utilizados pelo TERRA para assegurar que as páginas da web funcionem corretamente, para guardar as suas preferências (como linguagem ou tamanho da fonte selecionado por você), para conhecer a sua experiência de navegação e para compilar informações estatísticas anônimas(fonte: http://www.terra.es/aviso-legal/politica_cookies.htm). ou sem optar por uma navegação anônima, você compartilha com o TERRA o seu histórico de acesso de aplicações, sendo este armazenado por meio do emprego de tecnologias específicas para coleta de informações ("Identificadores Anônimos" e "cookies"). Este compartilhamento, entretanto, não abrange o armazenamento de dados ou informações pessoais suas, tais como: nome, endereço, e-mail, entre outros, mas tão somente proporciona a você uma interação com o Portal e serviços neste disponibilizados de acordo com suas escolhas de navegação, de forma que estas moldarão os serviços e anúncios oferecidos a você. Sendo assim, ao acessar as páginas do Portal e fazer uso dos Serviços do TERRA sem desabilitar tais tecnologias ("Identificadores Anônimos" e "cookies"), você expressamente escolhe este tipo de navegação voltado exclusivamente aos seus interesses e, portanto, autoriza o armazenamento de informações por meio destas tecnologias.

O maior problema é que o portal inverte a relação de exigência de prévio, livre e informado consentimento, pois ao invés de exigir este consentimento, na realidade, possibilita ao usuário bloquear tal captação.

Ao adotar esta política de atuação o portal desconsidera a vulnerabilidade técnica do consumidor, pois o usuário tradicional não necessariamente irá ter conhecimentos suficientes para modificar as configurações da sua navegação, e principalmente não deve ter a obrigação de fazê-lo, pois na realidade ele deve consentir para o fornecimento dos seus dados e não responsabilizar-se por não fornecê-los.

A Lei nº 8.078 de 11 de setembro de 1990 (Código de Defesa do Consumidor) afirma, em seu art. 39 inciso IV, ser uma prática abusiva do fornecedor "prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços" (BRASIL, 2014-f)

Quanto a esta temática Claudia Lima Marques (1998, p. 147-8) afirma que:

> Na vulnerabilidade técnica, o comprador não possui conhecimentos específicos sobre o objeto que está adquirindo e, portanto, é mais facilmente enganado quanto às características do bem ou quanto à sua utilidade, o mesmo ocorrendo em matéria de serviços. A vulnerabilidade técnica, no sistema do CDC, é presumida para o consumidor não-profissional, mas também pode atingir o profissional, destinatário final fático do bem.

Ainda, aparentemente o provedor tenta transferir a responsabilidade pela eventual capatção não consentida dos dados pessoais do internauta, a empresa responsável pelo

desenvolvimento e fornecimento dos navegadores de *Internet*, pois cada espécie de sistema poderá ter os procedimentos próprios para que a navegação anônima seja habilitada.

Esta transferência de responsabilidades, se prevista em uma cláusula contratual, esta seja nula de pleno direito na forma do art. 51, inciso III da Lei nº 8.078 de 11 de setembro de 1990 (Código de Defesa do Consumidor).

Mais uma vez surge o problema de o termo elencar determinadas informações como pessoais e sensíveis, pois ao fazê-lo deixa de proteger outras informações que também merecem proteção, uma vez que atualmente torna-se essencial a "percepção de que até as informações aparentemente mais inócuas podem, se integradas a outras, provocar danos ao interessado." (RODOTÀ, 2009, p. 36).

Esta tendência de conceber e elencar determinadas informações como pessoais, excluindo outras tantas de proteção, acabou por influenciar o Projeto de Lei nº 4.060 de 2012, que, como já visto, exclui do conceito de dado pessoal informações que possam potencialmente identificar determinado indivíduo.

Dentro deste trecho ainda é possível visualizar que o portal trabalha com a ideia de segmentação de comportamentos, pois afirma que as informações prestadas, quando o usuário optar por não realizar uma navegação anônima, serão utilizadas para moldar os serviços e anúncios oferecidos a ele.

Após estas previsões, o Aviso Legal (TERRA BRASIL, 2014-a) prevê que o "Terra" utilizará as informações pessoais que o usuário compartilhar:

> As informações que você compartilha com o TERRA têm como finalidade a gestão, administração, prestação, ampliação e melhoramento do Portal e dos Serviços. Além disso, considerando a possibilidade de o usuário moldar a sua navegação em relação aos dados que lhe são relevantes, a utilização das informações compartilhadas permite a autodeterminação de uso de informação pelo usuário. O TERRA poderá compartilhar os dados por você fornecidos com outras empresas do grupo TERRA ou terceiros parceiros, no Brasil ou exterior, sempre respeitando às finalidades adstritas ao seu compartilhamento, sendo certo que para tanto o TERRA solicitará sua prévia anuência. Além disso, o TERRA utilizará seus dados cadastrais fornecidos por meio de formulários eletrônicos disponibilizados no Portal e nos Serviços, para melhor direcionar a você conteúdo comercial, publicitário ou patrocinado, em suas páginas. Quanto às informações de acesso por você compartilhadas ao visitar o Portal TERRA e armazenadas por meio de "Identificadores Anônimos" ou de "cookies", estas também serão utilizadas com o intuito de aperfeiçoar o Portal e os serviços de acordo com as suas escolhas de navegação, bem como para gerar dados estatísticos gerais com finalidade informativa e comercial. Estas informações igualmente poderão ser compartilhadas com terceiros parceiros, no entanto, sem que sejam revelados nomes ou dados de sua navegação, da mesma forma, que caso você navegue em sites de parceiros, os registro de sua navegação nestes sites serão compartilhados por estes parceiros com o TERRA. Em havendo solicitação formal por qualquer autoridade pública, você está ciente de que o TERRA encaminhará seus dados pessoais, independente de notificação prévia.

Assim como o portal argentino, o portal brasileiro também refere que as principais finalidades da utilização dos dados pessoais dos usuários destinam-se a uma correta prestação dos serviços, sendo esta a justificativa mais recorrente. Todavia, nem sempre ela é verdadeira, pois não se pode esperar que os provedores de acesso à internet revelem ao consumidor o real objetivo da captação dos dados pessoais, já que o próprio termo afirma que estas informações pessoais também poderão servir para o desenvolvimento e oferta de outros serviços.

A referência de que a possibilidade de o usuário moldar a sua navegação em relação aos dados que lhe são relevantes, bem como que a utilização das informações compartilhadas, concede a ele uma autodeterminação do uso de suas informações, não estando completamente correta, pois na realidade a única escolha que cabe ao usuário é a navegação anônima ou não.

Não há qualquer previsão de que o usuário poderá acessar livremente as informações registradas, tampouco, que ele poderá retificá-las. Portanto efetivamente ele não molda a sua navegação, apenas opta por ela ser anônima ou não.

Também aparece a previsão de que o "Terra" poderá ceder os dados dos usuários a outras empresas pertencentes ao mesmo grupo econômico ou a terceiros, porém refere que sempre deverá ser respeitada a finalidade estrita do compartilhamento, bem como deverá ser recolhida anuência expressa do usuário. Contudo em momento algum o documento traz a definição destes terceiros, ou seja, às informações pessoais do internauta poderão se submetidas a tratamento por empresas sem que ele consinta e tampouco tenha conhecimento, o que atinge a autodeterminação informativa, pois reduz o seu controle sobre estes seus dados.

O documento (TERRA BRASIL, 2014-a) ainda excepciona do seu tratamento determinadas informações ao afirmar que: "Esta Política de Privacidade não se aplica aos conteúdos referentes a anúncios e links publicados por parceiros do 'TERRA'. Nesses casos, é imprescindível que você, ao acessar tais publicações, procure e leia a Política de Privacidade vinculada ao conteúdo por você acessado."

O Aviso sobre a proteção à privacidade (TERRA BRASIL, 2014-a) determina que o usuário tenha a sua disposição as seguintes opções quanto ao armazenatmento dos seus dados pelo "Terra":

> O compartilhamento dos seus dados é sempre uma escolha feita por você. Lembre-se que você pode desabilitar "cookies" antes da navegação ou mesmo realizar a navegação anônima. O TERRA adverte, no entanto, que alguns serviços poderão ser significativamente prejudicados ou até mesmo se tornarem inacessíveis, se você escolher não compartilhar seus dados de acesso ou informações pessoais.Quanto ao compartilhamento de informações de acesso por "Identificadores Anônimos" ou "cookies", caso este não seja de seu interesse, basta ajustar a

> configuração de seu navegador ou de seu dispositivo de acesso à Internet. Desta forma, será necessário que você efetue novo registro a cada vez que acessar um serviço que requeira um cadastro prévio, já que todos os Identificadores Anônimos (e não apenas os do TERRA) serão desabilitados do seu navegador.Você pode desabilitar o armazenamento de dados de duas formas: desabilitando os "cookies", o que pode limitar a sua navegação; ou realizando navegação anônima (os "cookies" e "identificares anônimos" serão excluídos após à sua visita ao site).

Neste trecho fica clara uma sensível diferença entre o tratamento dado pelo mesmo Portal de Internet em países que têm uma legislação específica de proteção de dados pessoais e aqueles que não legislaram especificamente quanto à matéria. Enquanto na Argentina o termo afirma expressamernte que não poderá haver qualquer distinção na prestação dos serviços decorrente da negativa do usuário em compartilhar os seus dados pessoais, no Brasil a previsão apresenta-se em sentido completamente oposto, afirmando que os serviços poderão ficar significativamente prejudicados caso o usuário não deseje compartilhar suas informações pessoais.

Esta exigência, além de violar regras de direito do consumidor[128], pois afeta o objeto de uma contratação consistente na prestação adequada e eficaz de um serviço, também viola o princípio de que o consentimento para o compartilhamento de dados pessoais deve ser livre. Não há que se falar em prévio e livre consentimento quando o usuário é alertado que os serviços remunerados que contratou poderão ser prejudicados, caso opte por não ceder ao portal de Internet seus dados pessoais.

O problema não é somente condicionar a prestação adequada dos serviços ao compartilhamento de dados pessoais pelo usuário, mas tratar de forma desigual usuários que optem por não compartilhar as suas informações pessoais.

O compartilhamento das informações deve ser uma faculdade do usuário. Ele deve ter liberdade de escolher se pretende disponibilizar ou não as suas informações pessoais àquela empresa, exercendo assim uma efetiva autodeterminação informativa, e esta faculdade deve ser exercida sem qualquer ônus para o invidíduo. Portanto, o exercício dessa faculdade não

---

[128] Tal previsão afronta o art. 6º incisos II e IV (BRASIL, 2014-f) que afirmam ser direito do consumidor: "a educação e divulgação sobre o consumo adequado dos produtos e serviços, assegurados à liberdade de escolha e a igualdade nas contratações" e "a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços".
Além disto, esta previsão na forma do art. 39 incisos V (BRASIL, 2014-f) pode ser considerada uma prática abusiva, pois o fornecedor esta exigindo "do consumidor vantagem manifestamente excessiva".
Caso esta previsão conste do contrato de fornecimento ela será nula de pleno direito na forma do art. 51 incisos IV, IX e XIII (BRASIL, 2014-f), pois ela "estabelece obrigação considerada iníqua, abusiva, que coloca o consumidor em desvantagem exagerada, sendo incompatível com a boa-fé ou a equidade", e ainda "deixa ao fornecedor a opção de concluir ou não o contrato, embora obrigando o consumidor".
Por fim, ela "autoriza o fornecedor a modificar unilateralmente o conteúdo ou a qualidade do contrato, após sua celebração".

pode condicionar ou prejudicar a prestação dos serviços que for contratada, pois na realidade os únicos dados que o internauta tem obrigação de fornecer são aqueles pertinentes ao contrato ou cadastro para o serviço.

Esta previsão do termo não se refere somente a estes dados, pois disciplina a questão da possibilidade de obtenção de informações pessoais através do sistema de *cookies*, e o compartilhamento das informações de navegação não pode ser considerado uma obrigação do usuário dos serviços de Internet.

Dentro da perpectiva de segurança dos dados pessoais, o portal (TERRA BRASIL, 2014-a) se posiciona perante o usuário no sentido de que:

> O TERRA se preocupa com a segurança das suas informações e, por isso, adota os níveis elevados de segurança de proteção de dados baseados nas melhores práticas adotadas pelo mercado, tomando todas as medidas necessárias para evitar a perda, mau uso, alteração, acesso não autorizado ou subtração indevida dos seus dados pessoais.. Alguns destes meios são as senhas de segurança e as criptografias utilizadas em seus servidores e nos dados trafegados.Apesar dos esforços empreendidos pelo TERRA a fim de garantir a segurança dos seus dados, a utilização de serviços e o acesso a conteúdos da Internet, envolve alguns riscos e exposições. Assim, é imprescindível você também faça a sua parte, tomando as seguintes medidas que podem reduzir os riscos envolvidos:

Esta previsão privilegia o princípio da segurança dos dados pessoais, o que deve ser entendido como uma obrigação do ente que capta e trata dados pessoais de terceiros, pois estes jamais serão de sua exclusiva propriedade. Porém se o usuário realmente contribuir para esta proteção, estará auxiliando na defesa dos seus próprios direitos fundamentais, e a utilização do Aviso legal como um documento educativo e de orientação neste sentido é algo elogiável.

Não obstante, esta previsão constitui-se em uma obrigação da empresa que presta tal serviço, pois ela explora e lucra com esta atividade econômica e, portanto, deve prestar a garantia de que este fornecimento ocorrerá de forma segura.

Este dever de segurança encontra previsão na Lei nº 8.078 de 11 de setembro de 1990 (Código de Defesa do Consumidor), que prevê em seu art. 6º inciso I ser direito do consumidor "a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos" (BRASIL, 2014-f).

Além disto, o inciso III estabelece que o usuário tem direito a "informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem" (BRASIL, 2014-f)

Por fim, o art. 8º do mesmo diploma legal estabelece que:

> Os produtos e serviços colocados no mercado de consumo não acarretarão riscos à saúde ou segurança dos consumidores, exceto os considerados normais e previsíveis em decorrência de sua natureza e fruição, obrigando-se os fornecedores, em qualquer hipótese, a dar as informações necessárias e adequadas a seu respeito (BRASIL, 2014-f).

Quanto a este dever de segurança Claudia Lima Marques (1998, p. 615) afirma que:

> O consumidor que adquire um produto ou utiliza um serviço oferecido no mercado brasileiro passa a ter, no sistema do CDC, dois tipos de garantia: a garantia legal da adequação do produto ou do serviço, a qual será concretizada através da utilização das novas normas sobre o vício e garantia de segurança razoável do produto, imposta pelo CDC nos arts. 8.º a 17, e que tem por fim a proteção da incolumidade física do consumidor e daqueles equiparados a consumidores.

Contudo estas orientações não podem servir como forma de se excluir ou minorar a responsabilidade que deve ter o ente que trata os dados pessoais dos usuários, pois o documento surge de uma fonte unilateral e não pode, sob pena de violação do princípio da boa-fé objetiva e dos deveres de lealdade e probidade, ser utilizado para afastar responsabilidades legais do ente que o produziu.

Quanto à possibilidade de personalização dos serviços prestados pelo "Terra", o Aviso Legal (TERRA BRASIL, 2014-a) preleciona que:

> Praticamente todo conteúdo que você acessa nos serviços do TERRA pode ser personalizados, muito embora, o TERRA disponibilize também a você serviços e notícias de interesse geral. Isso significa que ao invés de mostrar o mesmo conteúdo para todos os usuários, o TERRA pode construir um perfil baseado no seu histórico de acesso de aplicações, apresentando-lhe, além dos conteúdos e serviços de interesse geral, conteúdos e serviços mais próximos aos seus interesses. Isso ocorre em inúmeras situações: nas páginas do Portal, em comunicações eletrônicas, e em anúncios e publicidade apresentada a você. Em relação às publicidades personalizadas, caso você não opte por desabilitar cookies ou navegar de forma anônima, estas serão direcionadas a você, em razão de produtos observados em visitas a outros sites. Nesta situação, caso não seja de seu interesse recebê-las, você poderá desabilitar o banner da publicidade, clicando no ícone localizado no canto direito deste. Vale lembrar que somente as publicidades personalizadas conterão este ícone e esta possibilidade de desabilitação. A personalização é vantajosa, pois permite disponibilizar a você uma plataforma, que apesar de conter conteúdos de interesse geral, é modulada de forma a aproximar-se ao máximo de seus interesses e preferências.

Em mais uma oportunidade, o Termo de Política de Privacidade demonstra que a segmentação comportamental ocorre, pois reafirma que os conteúdos dos serviços do Portal "Terra", dentre os quais os serviços de provedor de acesso, podem ser personalizados. Ele o faz de forma a motivar os usuários a consentir com esta prática, evidenciando as vantagens de

submeter-se a este tratamento pessoalizado, porém desconsidera que os usuários podem optar por não participar desta forma de prestação dos serviços.

Contudo, a referência de que mesmo publicidades externas ao "Terra" poderão ser direcionadas aos usuários é preocupante, pois esta previsão enfraquece a aplicabilidade dos princípios da finalidade e do consentimento prévio e informado, e principalmente submete obrigatoriamente ao usuário geral, que não desabilita a navegação através de *cookies*, a uma infinidade de ações de *marketing* não consentidas.

É possível a compreensão de que o usuário estaria exercendo a sua autodeterminação informativa quando desabilita a navegação através dos *cookies*, ou realiza uma navegação anônima, porém estes procedimentos invertem a relação que deve ser estabelecida. A regra geral deve ser que sempre o acesso a dados pessoais de uma determinada pessoa (ou que possam identificar uma determinada pessoa) somente poderão ser captados, recolhidos ou tratados com o seu prévio, livre e informado consentimento, sendo excepcional o acesso a estes dados sem esta condição.

Portanto não é usuário que tem a obrigação de desabilitar eventual forma de navegação, mas os entes que operam os sistemas é que devem buscar estratégias de informar aos usuários qual será o tratamento a que os seus dados ficarão submetidos. O dever de informação é que precisa condicionar a captação dos dados, e não um procedimento técnico de responsabilidade do usuário titular.

2.4 COTEJO DA EFETIVIDADE DAS LEGISLAÇÕES PARA EVITAR A SEGMENTAÇÃO COMPORTAMENTAL NOS DOCUMENTOS INVESTIGADOS.

No decorrer da análise de cada um dos termos, constatou-se que eles apresentam previsões muito semelhantes, apesar de que a eficácia de cada um deles ficar adstrita a ordenamentos jurídicos que tratam de forma diferente a proteção de dados pessoais no ambiente virtual.

Por um lado, tanto Argentina quanto o Uruguai criaram legislações específicas que tratam da matéria da proteção de dados pessoais. Por outro lado, o Brasil até o Marco Civil da Internet contava com uma grande lacuna no tratamento da matéria. Porém, mesmo com a Lei nº 12.965 de 2014, persistem diversas questões pertinentes à proteção dos dados que não

foram regulamentadas ou cujas previsões legais deveriam receber uma reformulação para adequar-se à realidade informacional[129].

A mera existência de legislação específica não necessariamente gera termos de política mais protetivos ao usuário internauta, dado que em muitas ocasiões esta legislação pode flexibilizar, de forma indevida, princípios essenciais para um efetivo resguardo da privacidade do titular dos dados pessoais, tais como o da finalidade ou o da exigência de prévio consentimento.

No ordenamento brasileiro tramitava junto à Câmara dos Deputados o Projeto de Lei nº 4.060 de 2012, que, pelas suas previsões, em diversos pontos iria tornar o sistema brasileiro menos protetivo. Dentre estes, é possível citar a restritiva definição legal de dado pessoal e a completa ausência de regulamentação do direito ao acesso para internauta às informações constantes em arquivos no ambiente virtual, motivo pelo qual concorda-se com o seu arquivamento e com a abertura de novo processo de consulta popular para a elaboração da legislação específica para a proteção de dados pessoais (BLOG DO PLANALTO, 2015).

À sua maneira, as legislações do Uruguai e da Argentina trazem um completo sistema para o tratamento dos dados pessoais em arquivos, bancos ou registros digitais, e estas legislações inclusive são consideradas como tendo um sistema de proteção adequado no âmbito da União Européia.

Esta qualificação é extremamente relevante, tendo em vista que a União Européia foi pioneira ao estabelecer uma nova perspectiva de proteção da privacidade a partir da garantia da autodeterminação informativa, ou seja, por meio do controle pelo usuário de seus dados pessoais na captação, recolhimento ou tratamento.

Esta disparidade nos níveis de proteção reflete-se nos Termos de Política de Privacidade analisados. Enquanto o portal "Terra" na Argentina e no Uruguai disciplina por meio de um documento formal diversas regras e assume responsabilidades para a proteção da privacidade dos seus usuários, este mesmo ente não demonstra o mesmo esmero em face do internauta brasileiro.

O Termo de Política de Privacidade do "Terra" argentino traz, em um único documento, diversas obrigações a ambos os polos da relação jurídica de compartilhamento de

[129]Como exemplo destas questões que deveriam receber uma reformulação é possível citar o direito ao acesso, que no ordenamento jurídico brasileiro ainda persiste sendo regulamentado, a nível infraconstitucional, pela lei do *habeas data*, ou seja, pela Lei nº 9.507 de 1997, uma legislação estabelecida para o acesso aos bancos de dados físicos, tanto é que traz previsões extremamente restritivas quanto à identificação do reponsável pelo banco de dados.

informações pessoais. Além disto, são garantidos aos usuários os direitos ao acesso, à retificação, à supressão dos dados pessoais.

Em conseguinte, o "Terra" brasileiro divide o termo em dois documentos, referindo que pretende proteger a privacidade dos seus usuários no denominado "Termo de Uso" e remetendo as peculiaridades desta proteção a um segundo documento, denominado "Aviso Legal".

Os principais problemas surgem na forma como foi redigido este segundo documento, visto que se visualiza que foi produzido unilateralmente, com o intuito exclusivo de gerar obrigações ao usuário e isentar ou minorar as responsabilidades do próprio portal quando do compartilhamento de informações pessoais. Extrai-se do texto do "Aviso Legal" que ele não faz qualquer referência expressa ao direito do usuário acessar os seus dados pessoais, e consequentemente deixa de prever os direitos do titular retificá-los, atualizá-los ou simplemente suprimi-los quando entender pertinente. Com isso o internauta não consegue exercer de forma autônoma o controle sobre eles.

O teor do documento argentino permite que o usuário efetivamente demande do portal o respeito à sua autodeterminação informativa, o que não ocorre no termo do mesmo portal no Brasil.

Quanto à temática da presente pesquisa, a maior distinção entre os referidos documentos é que o termo disponibilizado na Argentina e no Uruguai, em decorrência das próprias legislações protetivas destes países, não visa convencer o usuário a submeter-se à segmentação comportamental, de modo que não insiste na oferta de serviços personalizados, tampouco relaciona as suas vantagens. Nestes países não há vedação ao usuário de submeter-se a segmentação comportamental, porém esta possibilidade não traz a mesma carga persuasiva que aquela constante no termo de privacidade brasileiro.

No termo de privacidade argentino, não há qualquer condicionamento da qualidade dos serviços prestados ao compartilhamento dos dados pessoias. Pelo contrário, é garantido ao usuário que a cessão das suas informações pessoais será sempre voluntária e não prejudicará a prestação adequada dos serviços contratados. Por outro lado, de forma inclusive abusiva sob o ponto de vista das normas consumeristas, o termo de privacidade brasileiro afirma que, caso o usuário opte por não compartilhar os seus dados, poderá sofrer significativos prejuízos aos seus serviços.

Após a análise dos três ordenamentos jurídicos que trazem diferentes graus de proteção aos dados pessoais do internauta, verifica-se que uma legislação específica e eficaz de proteção de dados pode influenciar as empresas a adotarem políticas de proteção à

privacidade mais precisas, honestas e leais ao usuário, primando pelo respeito à boa-fé objetiva nas relações virtuais.

CONCLUSÃO

A sociedade informacional, como estudada, surgida da reformulação e potencialização do sistema de produção capitalista, caraterizada principalmente pelo avanço do desenvolvimento e pela utilização massiva das Tecnologias Informacionais e Comunicacionais (TIC), após a revolução informacional da década de 70 do século XX, tem diversas características essenciais. Dentre elas se destaca uma tendência à exposição da personalidade individual, por intermédio da captação e do tratamento de dados pessoais digitais.

Esta sociedade tem outra característica que consiste na necessidade individual de integrar-se em redes de relacionamento, sejam redes eminentemente privadas como as redes sociais, ou mesmo redes de caráter público-privadas, como aquelas provenientes dos serviços de *Internet*. Para integrar-se nessas redes, o sujeito deve ser identificado ou ao menos identificável, e, portanto, deve ceder, em alguma medida, informações pessoais a respeito da sua personalidade.

As soluções apontadas pelo sistema jurídico tradicional para a proteção dos direitos fundamentais, em especial para a proteção da privacidade, tradicionalmente consistiram em uma atuação negativa, ou seja, no impedimento da violação. Porém, com o avanço da revolução informacional estas barreiras jurídicas tornam-se ineficazes, pois de um lado o indivíduo é influenciado culturalmente à autoexposição, e de outro lado a ele é exigido que compartilhe suas informações pessoais para integrar-se em redes e usufruir das vantagens oferecidas pelas tecnologias, como visto no primeiro capítulo.

Para responder a essa realidade desde a década de 80 a União Europeia tem investido em ações visando à proteção da privacidade do cidadão em suas comunicações, procurando garantir que o titular possa ter o controle das suas informações, concedendo acesso a terceiros somente quando lhe forem oportunizadas todas as informações pertinentes ao tratamento a que estes dados pessoais serão submetidos.

Essa preocupação inicial da União Europeia se justifica porque embora se saiba que a vigilância e o controle pelos entes estatais sobre os seus cidadãos, a partir de bancos de dados, arquivos ou registros, não é uma exclusividade da sociedade informacional, a utilização das TIC ampliou o rol de sujeitos capazes de realizá-lo, tornando a sua prática algo acessível inclusive a empresas privadas, com destaque para os provedores de acesso e portais de *Internet*, como o "Terra" que, dentre os grandes provedores de acesso à *Internet* no Brasil, tem abrangência nos países mercosulinos analisados.

Dentro deste contexto surge a segmentação de comportamentos através de dados pessoais digitais. A segmentação dos indivíduos com base na captação dos seus dados pessoais, como se verificou no primeiro capítulo, é inerente à sociedade informacional e origina-se em primeiro lugar de uma nova forma de *Marketing*, denominado *Marketing* de relacionamento, onde o vendedor consegue reduzir seus custos com publicidade ao estabelecer uma relação com os individuos que potencialmente têm uma grande possibilidade de consumir os seus produtos e serviços. Portanto, constatou-se que as empresas tentam vincular-se a uma determinada clientela através do acesso à personalidade dos seus potenciais consumidores, e este acesso é facilitado pelos dados pessoais dos indivíduos constantes em bancos, registros ou arquivos digitais.

Esta estratégia, além de reunir uma série de dados dos internautas, ainda se justifica sob o ponto de vista psicológico, pois tende a utilizar-se de mecanismos provenientes da Psicologia cognitivo-comportamental para induzir os consumidores através do acesso incessante a ofertas vinculadas a sua personalidade. Desta forma, a segmentação comportamental, conforme se verificou no segundo item do primeiro capítulo, fundamenta-se tanto no *marketing* de relacionamento quanto na Psicologia cognitivo-comportamental, e não necessariamente seria ilícita, inclusive podendo trazer algumas vantagens ao indivíduo.

As dificuldades surgem quando este usuário é submetido de forma inconsciente a estas práticas, perdendo o controle sobre o tratamento dos seus dados pessoais e fragilizando o seu direito fundamental à proteção da privacidade, o que suscita inúmeros problemas jurídicos. Diante dessa nova realidade e considerando que, ao contrário do Brasil, outros dois parceiros do Mercado Comum do Sul (MERCOSUL) já possuem legislação específica sobre a proteção de dados pessoais, questionou-se se o Marco Civil da Internet, recentemente aprovado no Brasil, e o Projeto de Lei de Proteção de Dados Pessoais analisado possuem mecanismos adequados se comparados com aqueles já desenvolvidos pela Argentina e pelo Uruguai.

Em desdobramento desse problema de pesquisa, questionou-se se a existência da legislação específica reflete satisfatoriamente na redação dos Termos de Política de Privacidade adotados pelo provedor de acesso Terra nos países investigados.

Para responder juridicamente de forma adequada a estas questões, optou-se, no segundo capítulo, por realizar a análise comparativa das legislações de proteção de dados pessoais da Argentina, do Uruguai e do Brasil, cotejando-as com dois Termos de Política de Privacidade, provenientes da mesma empresa, e disponibilizados nesses países.

Para subsidiar a comparação entre as diferentes legislações, houve a eleição de seis categorias conceituais, a saber: a) conceituação de dados pessoais e sua classificação/suas

espécies; b) regulamentação do uso do dado sensível; c) consentimento do usuário para captação e uso dos dados de acordo com a finalidade prevista; d) veracidade dos dados pessoais registrados; e) procedimentos para acesso e retificação de dados; f) órgão de controle.

Após a aplicação destas categorias sobre os textos legislativos, chegou-se à conclusão de que as leis de dados pessoais do Uruguai e da Argentina são mais protetivas aos internautas que as previsões que regulamentam a matéria no Brasil, que atualmente conta apenas com algumas previsões dispersas no Marco Civil da Internet e na Lei do *Habeas Data*.

Constatou-se também que o ordenamento jurídico brasileiro pretendia regulamentar especificamente a matéria através do Projeto de Lei nº 4.060 de 2012. Porém esse projeto, em vista das previsões que constam em sua minuta, deveria ser aprimorado para que não reduzisse excessivamente o grau de proteção do titular dos dados pessoais. O Projeto de Lei nº 4.060 foi arquivado em 31 de Janeiro de 2015, conforme informação constante no site da Câmara Federal, e o Ministério da Justiça abriu, em 28 de janeiro de 2015, consulta pública para a elaboração de um novo anteprojeto. Espera-se que esta iniciativa solucione as vicissitudes e problemas apontados no projeto de lei anterior, trazendo um nível de proteção adequado aos dados pessoais dos internautas.

O principal obstáculo é, como se constatou no decorrer da análise comparativa entre os ordenamentos jurídicos, para uma proteção adequada no sistema brasileiro, a falta de uma previsão específica que garanta ao titular a efetiva fruição do acesso a suas informações que constem em bancos, registros ou arquivos digitais, além de regulamentar as possibilidades de retificação, supressão, atualização e imposição de confidencialidade.

Somente garantido ao titular de forma ampla, precisa e clara o exercício do efetivo controle de suas informações pessoais é que ele verdadeiramente poderá exercer a sua autodeterminação informativa e fortalecer a proteção a sua privacidade, mesmo em face da sociedade informacional, pois somente desta forma a premissa de respeito à autodeterminação informativa, tratada no primeiro capítulo, será efetivamente respeitada.

Devido a esta distinção entre os níveis de proteção, constatou-se, na parte final do segundo capítulo, que os termos de política de privacidade nos países analisados tendem a refletir um desnível na proteção dos direitos do usuário internauta.

Nos países que contam com legislações específicas sobre a matéria e que trazem uma previsão clara do direito ao acesso e seus consectários, os termos tendem a ter um caráter de maior oficialidade e a gerar obrigações também ao provedor que os produziu. Dessa forma os termos se mostram mais protetivos ao titular, como ocorre com a Argentina e com o Uruguai,

conforme se verificou pela analise da *Política de Privacidad*, disponibilizada pelo portal "Terra" em ambos os países.

Contudo, quando se visualiza uma legislação esparsa quanto à matéria e que prevê de forma pouco clara o acesso às informações pessoais, os termos de política de privacidade tendem a ser pouco protetivos e não estabelecer responsabilidades muito claras aos provedores, esforçando-se mais em delegar obrigações aos próprios usuários, como no caso do Brasil, conforme averiguado no texto do documento "A sua privacidade é importante para o 'Terra'", disponibilizado pelo portal "Terra" no Brasil.

Visualiza-se, ainda, que os termos de política de privacidade em países que regulamentam especificamente a proteção de dados pessoais não tentam persuadir o usuário a submeter-se à segmentação de comportamentos de forma tão incisiva quanto aqueles termos disponibilizados em ordenamentos que não regulamentam especificamente a matéria, como constatado no caso brasileiro.

Desta forma é possível concluir que a existência de uma legislação adequada e específica quanto aos dados pessoais tende a gerar termos de política de privacidade mais protetivos ao usuário, e, portanto, protegem e fortalecem, de forma mais eficaz, os seus direitos fundamentais, dentre os quais a sua privacidade.

Na realidade, pela análise dos documentos selecionados, constatou-se que a autorregulamentação das empresas que intermediam os serviços de *Internet* tendem a realizar acaba por refletir no grau de proteção que as legislações estatais concedem ao cidadão internauta. Portanto a existência de uma legislação específica que trate, respeitando as suas peculiaridades, os dados pessoais em arquivos digitais é essencial como forma de proteger os cidadãos que usufruem destes direitos.

A existência de uma legislação pensada em outro contexto e para outras finalidades, como a Lei do *Habeas Data*, ou mesmo algumas previsões de caráter geral constantes no Marco Civil da Internet, não são suficientes para proteção jurídica dos dados pessoais digitais e não geram políticas de privacidade mais protetivas.

Verifica-se que o mesmo provedor, em determinado ordenamento que regulamenta especificamente a matéria, garante ao usuário um serviço adequado e de qualidade, independente da sua disposição em autorizar o tratamento dos seus dados pessoais. Em outros países cuja regulamentação específica inexiste, tendem a condicionar a qualidade do serviço prestado à disponibilização dos dados pessoais.

O avanço da utilização massiva das TIC é um fenômeno que traz consigo duas características essenciais que se refletem nos resultados do presente trabalho. Em primeiro

lugar, trata-se de uma profunda transformação social cujos efeitos ainda não foram completamente compreendidos, e, portanto os resultados desta dissertação ainda são parciais sob o aspecto temporal, pois ainda se vivencia um momento de transição nos temas que envolvem fenômenos da sociedade informacional. Destaque-se que estes resultados não refletem qualquer juízo positivo ou negativo da massificação do uso das tecnologias e tampouco pretenderam oferecer respostas exatas ou abordar o conteúdo de maneira exaustiva, pois se sabe que temas permeados de complexidade e ditados pela instantaneidade, como é o caso da proteção de dados pessoais no ambiente virtual, exigem constante acompanhamento e debate, cujos resultados são respostas provisórias e sem pretensão de generalizações.

Espera-se que, com vistas a estas conclusões, países que ainda não regulamentaram especificamente a matéria, a exemplo do Brasil, optem por fazê-lo, sendo que o recente arquivamento do Projeto de Lei de Proteção de Dados analisado e a criação de um grupo de estudos proposto pelo Ministério da Justiça, com o objetivo de produzir um novo anteprojeto de lei, surgem como demonstrativos de que talvez este caminho seja seguido.

Nesse contexto entende-se que, observadas as peculiaridades do Brasil e consideradas as contribuições dos atores sociais na produção desse novo anteprojeto, a regulação dos dados pessoais no Brasil não pode ignorar as experiências dos países parceiros do MERCOSUL, em especial aqueles que já foram considerados pela União Européia como tendo uma proteção de dados pessoais adequada, analisados no presente trabalho. Defende-se a posição de que conste no anteprojeto uma previsão expressa que garanta ao titular o direito ao acesso, retificação, atualização e exclusão de seus dados, respeitando-se a autodeterminação informativa dos titulares, assim como seja prevista uma instância administrativa, responsável tanto pela fiscalização da atuação dos provedores, quanto pelo recebimento e processamento de reclamações por parte do titular cujos dados foram violados.

Esse posicionamento não significa, por outro lado, que se atribua a solução de todos os problemas no tratamento dos dados pessoais à simples edição da legislação específica. Por certo a lei será um dos instrumentos que poderão contribuir para maior proteção da privacidade dos internautas, mas a maior efetividade da proteção exige que sejam conjugadas com outras ações de sensibilização dos atores sociais para este importante tema.

Nesse sentido mostra-se imperioso que os internautas tenham conhecimento que são objeto de segmentação comportamental e, em respeito ao princípio da boa-fé objetiva, possam optar em permanecer ou não na relação jurídica contratual, pois o desenvolvimento das tecnologias da informação e comunicação e as vantagens advindas de seu uso não podem

servir de justificativa para a violação de direitos fundamentais tão caros aos cidadãos, como o seu direito à privacidade e à autodeterminação informativa.

REFERÊNCIAS

ANATEL, **Norma 004/95**, aprovada pela Portaria n. 148, de 31 de março de 1995 do Ministério das Comunicações. Disponível em <http://www.anatel.gov.br/hotsites/Direito_Telecomunicacoes/TextoIntegral/ANE/prt/minicom_19950531_148.pdf> Acesso em: 15 de junho de 2014.

ANDERSON, Chris; **A cauda longa:** do mercado de massa para o mercado de nicho. Trad. SERRA, Afonso Celso da Cunha. 7ª Edição. Rio de Janeiro: Elsevier, 2006.

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. Tradução por Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ARGENTINA. Congresso da Nação. **Lei nº 25.326 de 04 de Outubro de 2000**. Lei da Proteção de Dados Pessoais, os direitos de habeas data e garantias constitucionais. Disponível em <http://www.infojus.gob.ar/documentDisplay.jsp?guid=123456789-0abc-defg-g99-44000scanyel&title=ley-de-proteccion-de-los-datos-personales> acesso em 29 de setembro de 2014.

ARGENTINA, **Constitución Nacional**. Disponível em <http://www.senado.gov.ar/deInteres>, acesso em 20 de dezembro de 2014-a.

AZEVEDO, Ana. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**. Os conceitos fundamentais e a construção do novo modelo. 1ª Edição. 3ª Tiragem. São Paulo: Saraiva, 2009.

BAUMAN, Zygmunt. **Medo líquido**. São Paulo: Jorge Zahar, 2008.

BECK, Aaron T; ALFORD, Brad A. **O Poder Integrador da Terapia Cognitiva**. Tradução Maria Cristina Monteiro. Porto Alegre: Artes Médicas Sul, 2000.

BECK, Judith S. **Terapia Cognitiva:** Teoria e Prática. Tradução Sandra Costa. Porto Alegre: Artes Médicas Sul, 1997.

BECK, Urlrich. **sociedadede Risco** - Rumo à outra modernidade. São Paulo: Editora 34, 2010.

BORGESIUS Frederik Zuiderveen. **Segmentação comportamental:** Do *Not Track* e o desenvolvimento jurídico europeu e holandês. Disponível em <http://www.politics.org.br/sites/default/files/poliTICs14_frederik_borgesius.pdf> Acesso em: 24 de fevereiro de 2014.

BRASIL. Assembléia Nacional Constituinte da república Federativa do. **Constituição da República Federativa do Brasil de 05 de Outubro de 1988**. Disponível em <

http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 15 de junho de 2014.

_____. **Lei nº 12.965 de 23 de Abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 29 de setembro de 2014-a.

_____.**Projeto de Lei nº 4.060 de 13 de junho de 2012**. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=5AC548E2DA55C77B90137A50E27027F8.proposicoesWeb2?codteor=1001750&filename=PL+4060/2012> , Acesso em 26 de setembro de 2014-b.

_____. **Lei Nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm> Acesso em 29 de setembro de 2014-c.

_____, **Rede Nacional de Pesquisa, Guia do Usuário Internet/Brasil, versão 2.0**, abril de 1996, Documento N º RNP / RPU / 0013 D, Código CI 005. Disponível em <http://www.rnp.br/_arquivo/documentos/rpu0013d.pdf>. Acesso em: 15 de junho de 2014-d.

_____. **Lei Nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm> acesso em 29 de setembro de 2014-e.

_____. **Lei Nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm> Acesso em 29 de Novembro de 2014-f.

_____. Supremo Tribunal Federal. **Direito constitucional e administrativo. Habeas data. Acesso a informações. Sistema SINCOR De Cadastro. Manifestação pela repercussão geral**. Recurso Extraordinário com Repercussão Geral Reconhecida nº 673.707 originário de Minas Gerais, disponível em <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28RE%24%2ESCLA%2E+E+673707%2ENUME%2E%29+OU+%28RE%2EPRCR%2E+ADJ2+673707%2EPRCR%2E%29&base=baseRepercussao&url=http://tinyurl.com/ar85nw2> acesso em 16 de março de 2015.

_____, Superior Tribunal de Justiça. **Administrativo e processual civil. Habeas data. Pretensão de acesso ao registro de procedimento fiscal - RPF. Inadequação da via eleita. Documento interno de uso privativo da receita federal, que contém o registro das atividades dos auditores fiscais.**. Recurso Especial nº 1411585 originário de Pernambuco, disponível em <http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&processo=1411585&b=ACOR&thesaurus=JURIDICO> acesso em 16 de março de 2015-A.

BLOG PLANALTO. **Marco Civil da Internet e proteção de dados serão debatidos pela sociedade**. Disponível em <http://blog.planalto.gov.br/assunto/ministerio-da-justica/>, acesso em 04 de fevereiro de 2015.

BUENO, Regiane Gonçalves Vieira; IKEDA, Ana Akemi. **Análise do comportamento e segmentação de consumidores de produtos e serviços bancários:** Um estudo exploratório. Disponível em <http://www.ead.fea.usp.br/tcc/trabalhos/Artigo%20-%20Regiane%20G.%20V.%20Bueno.pdf>. Acesso em: 24 de fevereiro de 2014.

CAMARA DOS DEPUTADOS, **Projeto de Leis e Outras Proposiões PL 4060/2015**. Disponível em <http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>, acesso em 04 de fevereiro de 2015.

CARBÓ, Alejandra M. Gils. **Régimen Legal de las Bases de Datos y Hábeas Data**. Buenos Aires: La Ley, 2001.

CARVALHO, Manuel da Cunha. O Conceito de Servidor em informática e suas implicações jurídicas *In* **Revista de Direito do Consumidor**, São Paulo: revista dos Tribunais, n. 39, lul/set 2001, p. 158-179.

CASTELLS, Manuel. **A Era da Informação:** Economia, sociedade e Cultura V. 01: sociedade em Rede. 14ª Reimpressão com novo Prefácio. Rio de Janeiro: Zahar, 2003-A.

_____. **A Era da Informação**: Economia, sociedade e Cultura V. 02: O Poder da Identidade. Rio de Janeiro: Zahar, 2003-B.

_____. **A Galáxia da *Internet***: reflexões sobre a *Internet*, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003-C.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Edições Almedina, 2005.

CGI.BR. Comitê Gestor da Internet no Brasil**. Atribuições**. Disponível em <http://www.cgi.br/atribuicoes/> Acesso em 29 de Novembro de 2014.

_____o CGI.br e o Marco Civil da Internet. Disponível em < http://www.cgi.br/media/docs/publicacoes/4/CGI-e-o-Marco-Civil.pdf> Acesso em 29 de novembro de 2014-a.

CETIC.BR. **Centro de Estudos sobre as Tecnologias da Informação e da Comunicação**. Resultado da pesquisa TIC Provedores 2011. Disponível em <http://op.ceptro.br/cgi-bin/cetic/tic-provedores-2011.pdf>. Acesso em: 21 de outubro de 2013.

CHATELET, François; DUHAMEL, Olivier; PISIER-KOUCHNER, Évelyne. **As Concepções Políticas do século XX:** história do pensamento político. Traduzido por: COUTINHO, Carlos Nelson de; KONDER, Leandro. Rio de Janeiro: Jorge Zahar, 1983

DAPKEVICIUS, Rubén Flores. **La nueva ley de habeas data en Uruguay nº 18331**. Disponível em <http://ijerda.bay.livefilestore.com.pdf> acesso em 23 de Outubro de 2014.

DAVIDOFF, Linda L. **Introdução à Psicologia**. Tradução Auriphebo Berrance Simões, Maria da Graça Lustosa. São Paulo: McGraw-Hill do Brasil, 1983.

DE LUCA, Cristina. **Seis dos 1934 provedores *Internet* do Brasil concentram 78% das conexões**, notícia disponível em <http://www.nic.br/imprensa/clipping/2011/midia1215.htm>. Acesso em: 21 de outubro de 2013.

DELPIANO, Hector. **Actualidad de La Protección de Los datos personales Y del habeas Data em El Uruguay**. In PALAZZI, Pablo A. (Director). **Derechos y nuevas tecnologías**. Derechos Personalíssimos. Buenos Aires: Ad-Hoc, 2003 (p. 403-580).

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo, Renovar, 2006.

DORON, Roland; PAROT, Françoise. **Dicionário de Psicologia**. São Paulo: Ed. Àtica, 2001.

DWORKIN, Ronald. **Levando os Direitos a Sério**. Tradução Nelson Boeira. São Paulo: Martins Fontes, 2011.

ESPANHA, **Constitución Española de 1978**. Disponível em <http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=15&fin=29&tipo=2>. Acesso em 15 de maio de 2014.

FÉRNANDES DELPECH, Horácio. **Internet e su problemática juridica**. 2ª Edição. Buenos Aires: Abeledo-Perrot, 2004.

FERREIRA, João Gabriel Lemos. Os Direitos da Personalidade em evolução: o direito ao esquecimento. In **Direito Civil**. Publicação do XXII Congresso Nacional do CONPEDI-UNICURITIBA. Disponível em < http://www.publicadireito.com.br/artigos/?cod=4a46fbfca3f1465a> Acesso em 29 de Novembro de 2014 (p. 94-120).

GLOBO. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA**, disponível em <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 30 de junho de 2014.

GONÇALVES, Maria Eduarda. **Direito da informação:** novos direitos e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003.

GONZALINI, Osvaldo Alfredo. **Derecho Procesal Constitucional**. Habeas Data, Proteccíon de datos personales: douctrina y jurisprudência. 2ª Edicion revisada e ampliada. Santa Fé: Rubinzal-Culzoni, 2011.

HESSE, Konrad. **A Força Normativa da Constituição**, tradução MENDES, Gilmar Ferreira. Porto Alegre: Sérgio Fabris, 1999.

HUXLEY, Aldous. **Admirável mundo novo**. São Paulo: Globo, 2009.

JESUS, Damásio de; MILAGRE, José Antônio. **Marco Civil da Internet:** Comentários à Lei n. 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014.

JUSTIÇA FEDERAL. **Enunciados aprovados na VI Jornada de Direito Civil**. Disponível em: <http://www.jf.jus.br/cjf/CEJ-Coedi/jornadas-cej/VI%20JORNADA1.pdf>. Acesso em 29 de novembro de 2014.

KAKU, William Smith. *Internet* e comércio eletrônico: pequena abordagem sobre a regulação da privacidade. In*:* ROVER, Aires José. **Direito, sociedadee Informática:** Limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, p. 81-93, 2000.

KAMINSKI, Omar. **Privacidade na *Internet***. In*:* ROVER, Aires José. **Direito, sociedadee Informática:** Limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, p. 94-103, 2000.

LEMOS, André. **A arte da vida:** diários pessoais e web cams na *Internet*. XI COMPÒS, Rio de Janeiro: ECO/UFRJ, 2002. Disponível em <http://www.portcom.intercom.org.br/pdfs/109986911192793762783072499970909167230.pdf>. Acesso em: 30 de junho de 2014.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de *Internet***. São Paulo: Editora Juarez de Oliveira, 2005.

_____. **Tutela e Privacidade na *Internet***. São Paulo: Saraiva 2012.

LÉVY, Pierre. **Cibercultura**. Lisboa: Piaget, 2005.

LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LOBO, Paulo Luiz Neto. **Constitucionalização do Direito Civil**. *In* FIUZA, César; DE SÁ, Maria de Fátima Freire; NAVES, Bruno Torquato de Oliveira Naves (coord.) **Direito Civil Atualidades**. Belo Horizonte: Del Rey, 2003.

LORENZETTI, Ricardo Luiz. **Fundamentos do Direito Privado**. São Paulo: Editora Revista dos Tribunais, 1998.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor**. O novo regime das relações contratuais. 3ª Edição Revisada, Atualizada e Ampliada. Sâo Paulo: Editora Revista dos Tribunais, 1998.

MARTINS-COSTA. Judith. **A boa-fé no Direito Privado Sistema e tópica no processo obrigacional**. 1ª Edição. 2ª Tiragem. São Paulo: Rt, 2000.

_____. **Os avatares do Abuso do direito e o rumo indicado pela Boa-Fé.** Disponível em <http://www.fd.ulisboa.pt/portals/0/docs/institutos/icj/luscommune/costajudith.pdf> acesso em 03 de setembro de 2014.

MASINA, Renato Hugo. **Análise da aceitação do recebimento de anúncios personalizados, através de smartphones, enquanto o usuário estiver dentro do shopping**. Trabalho de conclusão de curso de graduação do curso de Administração da Universidade Federal do Rio Grande do Sul. Disponível

em<http://www.lume.ufrgs.br/bitstream/handle/10183/87825/000911628.pdf?sequence=1> Acesso em: 24 de fevereiro de 2014.

MENDES, Gilmar, BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 9ª Edição. São Paulo: Saraiva, 2014.

METTELART, Armand. **História da sociedadeda Informação**. São Paulo: Loyola, 2002.

MOLON, Alessandro. **Comissão Especial destinada a proferir parecer ao Projeto de Lei nº lei nº 5.403, de 2001**, do Senado Federal que "dispõe sobre o acesso a informações da internet e dá outras providências' (PL 5403/01), 2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=50411FF5EE9F7AA87B17C9052C201B65.proposicoesWeb1?codteor=1012195&filename=Tramitacao-PL+5403/2001>. Acesso em 19 de novembro de 2014.

MORI, Michele Keiko. **Direito à Intimidade Versus Informática**. Curitiba: Juruá, 2002.

NALIN, Paulo Roberto Ribeiro. **Ética e Boa-Fé no Adimplemento Contratual**. *In* FACHIN, Luiz Edson (coord.) **Repensando Fundamentos do Direito Civil Contemporâneo**. Rio de Janeiro: Renovar, 1998.

NEGROPONTE, Nicholas. **A Vida Digital**. São Paulo: Companhia das Letras, 1995.

ORWELL, Georg. **1984**. São Paulo: Companhia das Letras, 2009.

PALAZZI, Pablo Andréas. **La proteccíon de datos personales en la Argentina**. 1ª Ed. Buenos Aires: Errepar, 2004.

PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2002.

PEPPERS, Don; ROGERS, Martha. **Privacidade e conflito:** Nos EUA, consumidores apelam ao governo para evitar que empresas usem informações capturadas na *Internet*, notícia disponível em <http://epocanegocios.globo.com/Revista/Epocanegocios/0,,EDR82804-8493,00.html>. Acesso em: 24 de fevereivo de 2014.

PEREIRA, Marcelo Cardoso. **Direito à Intimidade na *Internet***. 1ª Edição 3ª Tiragem. Curitiba: Juruá, 2005.

PÉREZ LUÑO, Antonio-Enrique**. Derechos humanos, estado de Derecho y Constitución**. 9. ed. Madri: Editorial Tecnos, 2005.

_____. ***Internet* y los derechos humanos**. In: Anuario de Derechos Humanos. Nueva Época. Vol. 12. 2011, p. 287-329. Disponível em: < http://revistas.ucm.es/index.php/ANDH/article/view/38107>. Acesso em: 08 março 2013.

PIZZINATTO, Andrea Kassouf; ZEM, Carlos Alberto; PIZZINATTO, Nadia Kassouf. **Do marketing de massa ao foco no cliente**. In: PIZZINATTO, Nadia Kassouf (org.) Marketing: Focado na cadeia de clientes. São Paulo: Atlas, p. 01-22, 2005.

PORTUGAL. **Constituição da República Portuguesa de 1974**. Disponível em <http://www.fd.uc.pt/CI/CEE/OI/Constituicao_Portuguesa.htm>. Acesso em: 15 de maio de 2014.

POULLET, Yves; PÉREZ ASINARI, Maria Verônica; PALAZZI, Pablo Andréas**. Derecho a La intimidad y a la protección de datos personales**. Buenos Aires: Heliasta, 2009.

POSER, Denise Von. **Marketing de Relacionamento:** maior lucratividade para empresas vencedoras. Barueri. SP: Manoele, 2005.

PULVIRENTI. Orlando D. **Derechos Humanos e Internet**. Buenos Aires: Errepar, 2013.

RAMOS, Pedro Henrique Soares. Uma questão de escolhas: o debate sobre a regulação da neutralidade da rede no marco civil da internet. In **Direito e Novas Tecnologias**. Publicação XXII Congresso Nacional do CONPEDI-UNINOVE. Disponível em < http://www.publicadireito.com.br/artigos/?cod=b750f74544cb00c1> Acesso em 29 de Novembro de 2014 (p. 266-291).

RIBEIRO, Joaquim de Sousa. **O imperativo de transparência no Direito Europeu dos Contratos**. *In* FIUZA, César; DE SÁ, Maria de Fátima Freire; NAVES, Bruno Torquato de Oliveira Naves (coord.) **Direito Civil Atualidades**. Belo Horizonte: Del Rey, 2003.

RIFKIN, Jeremy. **A Era do Acesso**. 2ª Edição. São Paulo: Makron, 2005.

RODOTÁ, Stefano; MORAES, Maria Cecília Bodin de. **A vida na sociedade da vigilância – a privacidade hoje**. São Paulo, Renovar, 2008.

ROTONDO, Felipe. **Flujo de información y sus limitaciones**. Disponível em < http://www.redipd.org/actividades/seminario_2010/common/ponencias/Seminario_junio_2010_Felipe_Rotondo.pdf> acesso em 23 de Outubro de 2014.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. **O direito à proteção dos dados pessoais:** uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro. Direitos Fundamentais e Justiça. n.11, abr./jun. 2010.

SARLET, Ingo Wolfgang. **A eficácia dos Direitos Fundamentais**. Uma Teoria Geral dos Direitos Fundamentais na Perspectiva Constitucional. 10ª Edição. Porto Alegre: Livraria do Advogado, 2009.

SIBILA, Paula. **O show do eu:** a intimidade como espetáculo. Rio de Janeiro: Nova Fronteira, 2008.

_____. **Os diários íntimos na *Internet* e a Crise da Interioridade Psicológica**. In: LEMOS, André; CUNHA, Paula (orgs.). Olhares sobre a Cibercultura. Porto Alegre: Sulina, p. 139-152, 2003.

SILVA, Beronalda Messias da. Marco civil da internet: o que muda com relação aos cookies de internet? In **Direito e Novas Tecnologias**. Publicação XXII Congresso Nacional do

CONPEDI-UNINOVE. Disponível em < http://www.publicadireito.com.br/artigos/?cod=7d806dddbe08d7be> Acesso em 29 de Novembro de 2014 (p. 250-265).

SILVA, Clóvis do Couto**. A obrigação como um processo**. Reimpressão. Rio de Janeiro: Editora FGV, 2006.

SILVA, Edson Ferreira da. **Direito à Intimidade:** de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código Civil de2002. 2. Ed. rev. atual. ampliada São Paulo: Juarez de Oliveira, 2003.

SILVA, Rosane Leal. As tecnologias da informação e comunicação e a proteção de dados pessoais. In: **Anais do XIX Encontro Nacional do CONPEDI**, 2010, Fortaleza. Anais. Fortaleza, 2010 (p. 3907-3918).

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 28ª Edição. São Paulo: Malheiros, 2007.

STRATTON, Peter; HAYES, Nicky. Dicionário de Psicologia. São Paulo: Ed. Pioneira Psicologia, 1994.

SUNSTEIN, Cass. **Republic.com**. Princeton: University Press, 2001.

KAZMIERCZAK, Luiz Fernando. Responsabilidade Civil dos Provedores De Internet *In* **Anais do XIX Encontro Nacional do CONPEDI-FUMEC**. Belo Horizonte, 2011 (p. 467-486). Disponível em <http://www.conpedi.org.br/manaus/arquivos/anais/bh/luiz_fernando_kazmierczak.pdf> Acesso em 29 de Novembro de 2014.

TEPEDINO, Gustavo. **Problemas de Direito Civil-Constitucional**. Rio de Janeiro: Renovar, 2001.

TELLINI, Denise Estrella. **Regime de direito internacional privado na responsabilidade dos provedores de internet.** Porto Alegre: Sergio Antônio Fabris, 2006.

TERRA ARGENTINA. **Política de Privacidade**. Disponível em <http://www.terra.com.ar/avisolegal/privacidad.htm> acesso em 29 de setembro de 2014.

TERRA BRASIL. **Termo de uso do portal TERRA**. Disponível <http://www.terra.com.br/avisolegal/> acesso em 29 de setembro de 2014.

_____. **Aviso Legal. Sua Privacidade é muito importante para o "TERRA"**. Disponível <http://www.terra.com.br/avisolegal/privacidade.html> acesso em 29 de setembro de 2014-a.

UNIÃO EUROPEIA. **Convenção para proteção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal**. Diretiva 108 de 1980. Disponível em <http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm> acesso em 15 de maio de 2014.

_____. **Diretiva 24 de 2006 do Parlamento Europeu e do Conselho da Europa relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE.** Disponível em<http://www.anacom.pt/render.jsp?contentId=963466v>. Acesso em: 15 de maio de 2014-a

_____. **Diretiva 46 de 1995 do Parlamento Europeu e do Conselho da Europarelativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML>.Acesso em: 15 de maio de 2014-b.

_____. **Diretiva 58 de 2002 do Parlamento Europeu e do Conselho da Europa relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)**. Disponível em <http://www.inst-informatica.pt/legislacao-e-directivas/identidade-e-seguranca-informatica/DIRECTIVA.pdf/view?searchterm=electr%C3%B3nico>.Acesso em: 15 de maio de 2014-c.

_____. **Diretiva 66 de 1997 do Parlamento Europeu e do Conselho da Europa relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações** Disponível em <http://www.anacom.pt/render.jsp?contentId=972449>. Acesso em: 15 de maio de 2014-d.

_____, Comissão da.**Grupo de Proteção de Dados Pessoais. Parecer nº 4/2002**. Disponível em <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_pt.pdf> acessado em 23 de outubro de 2014-e.

_____, Comissão. **Grupo de Proteção de Dados Pessoais. Parecer nº 6/2010**. Disponível em <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_pt.pdf > acessado em 23 de outubro de 2014-f.

URUGUAI, Congresso Nacional da República Oriental do. Lei nº 18.331 de 11 de Agosto de 2008. Proteção de dados pessoais e ação de "habeas data". Disponível <http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Anchor=> acesso em 29 de setembro de 2014.

VIDHYANATHAN, Siva. **A googlelização de tudo**. São Paulo: Cultrix, 2011.

VIRILIO, Paul. **A bomba informática**. Traduzido por Luciano Vieira Machado. São Paulo, SP: Estação Liberdade, 1999.

VOGAS, Rosíris Paula Cerizze; NEUMAYR, Rafael. A responsabilidade civil dos provedores de hospedagem por “perfis falsos” na internet *In* **Anais do XVIII Encontro Nacional do CONPEDI-CESUMAR**, Maringá, 2009 (p. 3959-3982). Disponível em < http://www.conpedi.org.br/anais/36/13_1210.pdf> Acesso em 29 de Novembro de 2014.

WRIGHT, Jesse H; BASCO, Monica R; THASE, Michael E. **Aprendendo a Terapia Cognitivo-Comportamental**. Tradução Monica Giglio Armando. Porto Alegre: Artmed, 2008.